UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA

v. 11 CR 623 (JG)

AGRON HASBAJRAMI,

Defendant.

----------X

GOVERNMENT'S MEMORANDUM IN SUPPORT OF ITS MOTION FOR AN *EX PARTE, IN CAMERA* REVIEW TO DETERMINE THE LEGALITY OF COLLECTION PURSUANT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AND IN OPPOSITION TO DEFENDANT'S MOTIONS TO SUPPRESS EVIDENCE OBTAINED OR DERIVED FROM SECTION 702 OF THE FISA AMENDMENTS ACT AND TO COMPEL DISCOVERY OF FISA APPLICATIONS, ORDERS AND RELATED MATERIALS AND MATERIALS RELATED TO THE SECTION 702 COLLECTION

REDACTED, UNCLASSIFIED VERSION

Loretta E. Lynch
United States Attorney
Eastern District of New York

Seth D. DuCharme
Matthew S. Amatruda
Saritha Komatireddy
Assistant U.S. Attorneys
Eastern District of New York

JOHN CARLIN
Assistant Attorney General
for National Security

Danya Atiyeh
Kiersten Korczynski
Trial Attorneys,
Counterterrorism Section,
Department of Justice
(Of Counsel)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

I. INTRODUCTION[1]

The government is filing this unclassified version of its classified memorandum in opposition to Defendant Agron Hasbajrami's ("Hasbajrami") Motions No. 1, 2, and 5 contained in his Pretrial Omnibus Motions and Incorporated Memorandum of Law in Support Thereof, which was filed November 27, 2014 (hereinafter "defendant's motions").[2] (Criminal Docket No. ("Dkt.") 11-623 (S-1)(JG)). This unclassified memorandum and the classified memorandum are also submitted to support the government's motion, pursuant to 50 U.S.C. §§ 1806(f) and 1825(g), that the Court (1) conduct an *in camera* and *ex parte* review of the applications, orders and other materials related to the collection pursuant to Title I (electronic surveillance, 50 U.S.C. §§ 1801-1812) and Title III (physical search, 50 U.S.C. §§ 1822-1829) of the Foreign Intelligence Surveillance Act ("FISA") (hereinafter "traditional FISA") from which evidence to be used at trial is obtained or derived; (2) find that the information at issue was lawfully acquired and that the electronic surveillance and physical searches were conducted in conformity with an order of authorization or approval; and (3) order that none of the materials be disclosed to the defense, and instead, that they be maintained by the United States under seal. For the reasons set forth below, the Court should deny the defendant's motion in its entirety and grant the government's motion.

A. OVERVIEW

In essence, the defendant's motions (1) seek suppression of all evidence obtained or derived from surveillance conducted pursuant to Section 702 of the FISA Amendments Act of 2008 ("FAA" or "Title VII"), codified at 50 U.S.C. § 1881a; and (2) renew the same discovery requests that this Court previously denied in the Section 2255 proceeding, seeking disclosure of classified

[1] [CLASSIFIED INFORMATION REDACTED]

[2] The government's responses to defendant's motions no. 3, 4, and 6-12 will be filed separately.

factual information relating to the Title I/III and Section 702 collection relevant to his case, including (a) all FISA applications, orders and related materials and their content (collectively, the "FISA materials"), (b) records and documents relating to the government's acquisition, use, and dissemination of his communications acquired pursuant to Section 702 (collectively, the "Section 702 materials"), and (c) the government's opinion of the legality of the Section 702 collection.

The defendant's motions for suppression and discovery were filed in response to the government's supplemental notification, provided on February 24, 2014, that, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), the government intended to offer into evidence or otherwise use or disclose in proceedings in Hasbajrami's criminal case information derived from acquisition of foreign intelligence information conducted pursuant to Section 702 ("Supplemental Notification"). Section 702 permits the targeting of non-U.S. persons reasonably believed to be located outside the United States, in order to acquire foreign intelligence information, subject to certain statutory requirements. *See* 50 U.S.C. § 1881a. The Supplemental Notification was provided based on a post-plea determination by the Department of Justice and the prosecutors that certain evidence or information obtained or derived from FISA Title I and Title III collection was itself also derived from other collection pursuant to Section 702 as to which Hasbajrami was aggrieved.

[CLASSIFIED INFORMATION REDACTED]

The defendant's motions have triggered this Court's review of the relevant Section 702 materials pursuant to 50 U.S.C. §§ 1881e(a) and 1806(f) to determine whether the Section 702 intelligence collection at issue herein was lawfully authorized and conducted in accordance with the requirements of the FAA. In addition, because the defendant's motion No. 5 seeks discovery of FISA materials, see Def. Mot. at 68, the government requests the Court conduct a review of the relevant FISA materials pursuant to 50 U.S.C. §§ 1806(f) and 1825(g) to determine whether the

FISA collection from which the evidence at trial was obtained or derived was lawfully authorized and conducted in accordance with FISA.[3]

As explained below, this Court should conduct an *in camera, ex parte* review of the Section 702 and FISA materials, in accordance with the provisions of 50 U.S.C. §§ 1806(f), 1825(g), and 1881e(a). Section 1806(f) provides that, where the Attorney General certifies that "disclosure or an adversary hearing would harm the national security of the United States, a district court "shall, notwithstanding any other law. . . review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f); *see also* 50 U.S.C. § 1825(g). This same procedure applies to motions to disclose Section 702-related materials or to suppress information obtained or derived from Section 702 acquisitions, which is deemed to be electronic surveillance conducted pursuant to Title I of FISA for purposes of such motions. 50 U.S.C. § 1881e(a). The Attorney General has filed such a declaration in this case.[4] Once the Attorney General files a declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other

---

[3] Section 1806(f) provides in pertinent part that the district court's review of the legality of FISA collection is triggered "[w]henever any motion or request is made by an aggrieved person pursuant to any other statute or rule . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discovery, obtain, or suppress evidence or information obtained or derived from electronic surveillance under [FISA]." *See also* 50 U.S.C. § 1825(g). Ordinarily, out of judicial economy, district courts conduct such a review only after receiving a motion to suppress FISA evidence, even where a prior motion for discovery has been filed. Since, however, the defendant has declined to seek suppression of the FISA evidence, the government accordingly requests that the Court conduct the requisite review.

[4] The Declaration and Claim of Privilege of the Attorney General of the United States is being publicly filed as part of this redacted, unclassified submission, and is being served on the defendant. *See* Exhibit 1.

materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f).

In opposition to the defendant's motions and in support of its motion, the government submitted a classified memorandum of law for the Court's *in camera, ex parte* review. This redacted version of that memorandum, from which all classified information, and all header, footer, and paragraph classification markings have been redacted, is also being publicly filed and served on the defendant.[5]

[CLASSIFIED INFORMATION REDACTED]

The unclassified documents have been electronically filed in the public docket. All of the classified documents and the original Attorney General's Declaration and Claim of Privilege have been submitted to the Court in a Sealed Appendix to the *in camera, ex parte* Memorandum for the Court's review, and the AG Declaration and Claim of Privilege will be attached to this redacted, unclassified filing and made publicly available.

The government expects that the Court will conclude from its *in camera, ex parte* review that: (1) the acquisition, retention, and dissemination of foreign intelligence information pursuant to the FAA and the FISA electronic surveillance and physical searches at issue in this case were all lawfully authorized and conducted; (2) the FAA complies with the Fourth Amendment and Article III of the U.S. Constitution; (3) the fruits of the FISA and FAA collection at issue should not be suppressed; (4) disclosure to the defendant or cleared defense counsel of the Section 702 and FISA materials and the Government's classified submission is not authorized because the Court can make an accurate determination of the legality of the surveillance and searches without disclosing such materials or portions thereof; and (5) the defendant's other discovery requests should be denied.

[5] As a result of the redactions, the pagination and footnote numbering of the classified *in camera, ex parte* memorandum and the redacted unclassified memorandum are different.

B. BACKGROUND

1. The Criminal Case

Hasbajrami's case arose from an investigation by agents of the Joint Terrorism Task Force ("JTTF"), which revealed that between April 2, 2011 and August 28, 2011, Hasbajrami communicated with a Pakistan-based extremist who informed Hasbajrami that he was part of a terrorist organization that engaged in attacks on American soldiers in Afghanistan. In addition, the individual promoted violent extremist activity through Internet communications and publications, and solicited funds that he represented would be used to support terrorist operations.

During the course of their communications, Hasbajrami sent approximately $1,000 to the extremist to support Islamic fundamentalist terrorist operations. In addition, Hasbajrami and the extremist planned for Hasbajrami's travel from New York to the Federally Administered Tribal Areas ("FATA") of Pakistan, where Hasbajrami hoped to join a jihadist fighting group. During their communications, Hasbajrami discussed with the extremist his desire to "marry with the girls in paradise," that is, to die as a martyr while engaged in fighting a holy war.

The government introduced a cooperating source ("CS") to Hasbajrami through online communications in order to determine whether Hasbajrami remained intent on supporting terrorism and joining a foreign fighter group abroad. Through the use of the CS, the government learned that Hasbajrami was continuing to make efforts to support international terrorism, and in fact was pursuing his plans to travel from the United States to the FATA to join a foreign fighter group.

On September 6, 2011, JTTF agents arrested Hasbajrami at John F. Kennedy International Airport in Queens, New York, from where he was about to travel to Turkey en route to Pakistan. Following his arrest and after waiving his Miranda rights, Hasbajrami made detailed statements to agents regarding his offense conduct.

[CLASSIFIED INFORMATION REDACTED]

On September 8, 2011, a grand jury in this District returned an indictment charging Hasbajrami with one count of providing material support to terrorists, in violation of 18 U.S.C. § 2339A(a). On September 13, 2011, the government filed notice of its intent to use or disclose, in the prosecution of Hasbajrami, information obtained or derived from electronic surveillance (Title I) and physical search (Title III) conducted pursuant to FISA, 50 U.S.C. §§ 1801-1812, 1821-1829. Thereafter, the government produced in discovery inculpatory evidence, including email communications that had been obtained pursuant to FISA. On January 26, 2012, the grand jury returned a superseding indictment, which included three additional counts of providing and attempting to provide material support, consisting principally of money (some of which was to be used for weapons) and personnel, all in violation of the same statute.

On April 12, 2012, Hasbajrami pleaded guilty to Count Two of the superseding indictment, which charged him with attempting to provide material support to terrorists in violation of 18 U.S.C. § 2339A(a). At sentencing on January 8, 2013, the Court imposed a sentence of the statutory maximum 15 years' imprisonment. Following the imposition of the sentence, Hasbajrami filed a *pro se* "motion to vacate, set aside, or correct" his conviction and sentence. On December 4, 2013, the Court deemed this a motion under Section 2255 in case number 13 CV 6852.

Thereafter, as explained in the government's previous filings, the Department determined that information obtained or derived from Title I or Title III FISA collection may, in particular cases, also be derived from prior Title VII collection, such that notice concerning both Title I/III and Title VII collections should be given in appropriate cases with respect to the same information. Following this determination, upon reviewing the evidence obtained or derived from Title I or Title III FISA collection in Hasbajrami's case and determining that certain evidence was

itself also derived from other collection pursuant to Section 702 as to which Hasbajrami was aggrieved, the government provided a Supplemental Notification stating that, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), the government intended to offer into evidence or otherwise use or disclose in proceedings in Hasbajrami's criminal case information derived from acquisition of foreign intelligence information conducted pursuant to Section 702, 50 U.S.C. § 1881a (ECF No. 65).

On September 12, 2014, this court heard argument on a number of the defendant's discovery requests, which were denied on the record, and directed the defendant to file a letter indicating whether he wished to withdraw his guilty plea. On September 20, 2014, the defendant filed a letter confirming his intent to withdraw his plea, and on October 2, 2014, this court issued an order withdrawing Hasbajrami's prior guilty plea and reopening the criminal case. On November 26, 2014, Hasbajrami filed the instant omnibus motion.

2. Overview of the FAA Collection at Issue

[CLASSIFIED INFORMATION REDACTED]

C. OVERVIEW OF FISA AND THE FISA AMENDMENTS ACT

1. The Foreign Intelligence Surveillance Act

Since the founding of this country, the government has relied on foreign intelligence collection to protect the nation. For the majority of that time and through the present day, much of this intelligence gathering has been conducted under the President's constitutional authority over national security and foreign affairs, with methods of surveillance evolving over time in light of developing technologies. Presidents have authorized warrantless wiretaps for foreign intelligence purposes since at least 1940. *See, e.g.*, *United States v. U. S. District Court for E.D. of Mich.*, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson).

In 1978, Congress enacted FISA "to regulate the use of electronic surveillance within the United States for foreign intelligence purposes." *See* S. Rep. No. 95-604, at 7 (1977). The statute was a response to congressional investigations into abuses of surveillance directed at specific American citizens and political organizations. *Id.* at 7-8. FISA was designed to provide a check against such abuses by placing certain types of foreign intelligence surveillance under the oversight of the FISC.[6]

FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical searches when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISC of Review"), which is composed of three United States District or Circuit Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b).

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act").[7] One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. 50 U.S.C. § 1804(a)(6)(B).

---

[6] The judges which sit on the FISC are Article III judges with life tenure that serve by designation of the Chief Justice of the United States. 50 U.S.C. § 1803(a).

[7] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[CLASSIFIED INFORMATION REDACTED]

a. The FISA Application

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance, physical searches, or both, within the United States where a significant purpose is the collection of foreign intelligence information.[8] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, "[f]oreign intelligence information" means:

> (1) information that relates to, and if concerning a United States person[9] is necessary to, the ability of the United States to protect against—
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> >
> > (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –
>
> > (A) the national defense or the security of the United States; or
> >
> > (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e); *see also* 50 U.S.C. § 1821(1), adopting the definitions from 50 U.S.C. § 1801. With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical searches may be conducted.

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

---

[8] [CLASSIFIED INFORMATION REDACTED]

[9] [CLASSIFIED INFORMATION REDACTED]

(1) the identity of the federal officer making the application;

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures to be followed;

(5) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(6) a certification, discussed below, of a high-ranking official;

(7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;

(8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and

(9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance except that an application to conduct a physical search must also contain a statement of the facts and circumstances that justify an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from" the target. 50 U.S.C. §§ 1823(a)(1)-(8), (a)(3)(B), (C).

b. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking executive branch official with national security responsibilities that:

(A) the certifying official deems the information sought to be foreign intelligence information;

> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also* 50 U.S.C. § 1823(a)(6).

c. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical searches, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1), 1821(4)(A).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is

about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c).

[CLASSIFIED INFORMATION REDACTED]

d. Attorney General's Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical searches, or both, before they are presented to the FISC.

2. The FISC's Orders

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance, physical searches, or both, only upon finding, among other things, that:

> (1) the application has been made by a "Federal officer" and has been approved by the Attorney General;
>
> (2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power (or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power);
>
> (3) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) and 50 U.S.C. § 1821(4) (physical search);
>
> (4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; and
>
> (5) if the target is a United States person, that the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

(U) FISA defines "foreign power" to mean –

(1) a foreign government or any component, thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. §§ 1801(a)(1)-(7); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means –

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

> (E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

any person who –

> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

50 U.S.C. §§ 1801(b)(1) and (2); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical searches, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *United States v. Rosen*, 447 F. Supp. 2d 538, 549-50 (E.D. Va. 2006); *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999). Additionally, FISA provides that "[i]n determining whether or not probable cause exists . . . a

judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC has made all of the necessary findings and is satisfied that the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical searches, or both, requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify:

> (1) the identity, if known, or a description of the specific target of the collection;
>
> (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched;
>
> (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search;
>
> (4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted;
>
> (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and
>
> (6) the applicable minimization procedures.

50 U.S.C. §§ 1805(c)(1) and 2(A); 1824(c)(1) and 2(A).

Under FISA, electronic surveillance or physical searches targeting a United States person may be approved for up to ninety days, and those targeting a non-United States person may be approved for up to one-hundred and twenty days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1).[10] Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. An extension for electronic surveillance or physical searches targeting a

[10] [CLASSIFIED INFORMATION REDACTED]

United States person may be approved for up to ninety days, and one targeting a non-United States person may be approved for up to one year.[11] 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

3. The Protect America Act and the FISA Amendments Act of 2008

In FISA, Congress limited the definition of the "electronic surveillance" governed by the statute to four discrete types of domestically-focused foreign intelligence collection activities. *See* 50 U.S.C. § 1801(f). Specifically, Congress defined "electronic surveillance" to mean (1) the acquisition of the contents of a wire or radio communication obtained by "intentionally targeting" a "particular, known United States person who is *in the United States*" in certain circumstances; (2) the acquisition of the contents of a wire communication to or from a "person *in the United States*" when the "acquisition occurs in the United States"; (3) the intentional acquisition of the contents of certain radio communications when the "sender and all intended recipients are located *within the United States*"; and (4) the installation or use of a surveillance device "*in the United States*" for monitoring or to acquire information other than from a wire or radio communication in certain circumstances. *Id.* (emphasis added); *cf.* 50 U.S.C. § 1801(i) (defining "United States person" to mean, as to natural persons, a citizen or permanent resident of the United States).

Because of FISA's definition of "electronic surveillance," FISA as originally enacted did not apply to the vast majority of surveillance the government conducted outside the United States. This was true even if that surveillance might specifically target U.S. persons abroad or incidentally acquire, while targeting third parties abroad, communications to or from U.S. persons or persons located in the United States. *See* S. Rep. No. 95-701, at 7 & n.2, 34-35 & n.16 (1978).[12]

---

[11] The FISC retains the authority to review, before the end of the authorized period of electronic surveillance or physical searches, the Government's compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

[12] Executive Order No. 12333, as amended, addresses, *inter alia*, the government's "human and technical collection techniques . . . undertaken abroad." Exec. Order No. 12333, § 2.2, 3 C.F.R. §

Congress was told in the hearing leading to FISA's enactment that the acquisition of international communications at the time did not rely on the four types of "electronic surveillance" covered by the definitions in the proposed legislation – including wire interceptions executed in the United States – and thus those operations would not be affected by FISA. *See Foreign Intelligence Surveillance Act: Hearing before the Subcomm. on Criminal Laws and Procedures of the S. Judiciary Comm.*, 94th Cong., 2nd Sess., at 11 ("Mar. 29, 1976 FISA Hrg.").[13] Congress heard similar testimony from other witnesses.[14] Accordingly, at the time FISA was enacted, Congress understood that most foreign-to-foreign and international communications fell outside the definition of "electronic surveillance." *See* S. Rep. 95-701, at 71 ("[T]he legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency."). Where the government did not intentionally target a particular, known U.S. person in the United States, FISA allowed the government to monitor international communications through radio surveillance, or wire

---

210 (1981 Comp.), *reprinted as amended in* 50 U.S.C. § 401 note (Supp. II 2008). That Executive Order governs the intelligence community, *inter alia*, in collecting "foreign intelligence and counter-intelligence" abroad, collecting "signals intelligence information and data" abroad, and utilizing intelligence relationships with "intelligence or security services of foreign governments" that independently collect intelligence information. *Id.* §§ 1.3(b)(4), 1.7(a)(1), (5) and (c)(1).

[13] Attorney General Levi subsequently elaborated: "The bill does not purport to cover interceptions of all international communications where, for example, the interception would be accomplished outside of the United States, or, to take another example, a radio transmission that does not have both the sender and all intended recipients within the United States." *Electronic Surveillance within the United States for Foreign Intelligence Purposes: Hearings before the Subcomm. on Intelligence and the Rights of Americans of the S. Select Comm. on Intel.*, 94th Cong., 2nd Sess., 180-81 (1976).

[14] *See, e.g., Foreign Intelligence Surveillance Act: Hearings before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 94th Cong., 2nd Sess. 8 (1976) (statement of former Justice Department official Philip Lacovara) ("[N]ot covered [under the bill] are international wire communications since it is relatively simple, I understand, to intercept these communications at a point outside the United States. Similarly, * * * the bill would have no application whatsoever to international radio traffic."); Mar. 29, 1976 FISA Hrg. 31 testimony of Morton Halperin) (stating that "if I am an American citizen [in the United States] and I make a phone call to London, and the Government picks it up on a transatlantic cable under the ocean, it is not covered," and "if it goes by microwave, or if it passes through Canada, it would not be covered").

surveillance of transoceanic cables offshore or on foreign soil, outside the statute's regulatory framework.

In 2006, Congress began considering proposed amendments to FISA aimed at modernizing the statute in response to changes in communications technology since its original enactment. *See Modernization of the Foreign Intelligence Surveillance Act: Hearing before the H. Permanent Select Comm. on Intelligence,* 109th Cong., 2nd Sess. (2006). Congress took up the issue concurrently with an inquiry into the Terrorist Surveillance Program ("TSP") – a program authorized by the President after the terrorist attacks of September 11, 2001, which allowed the NSA to intercept communications into, and out of, the United States where the government reasonably believed that a communicant included a member or agent of al Qaeda or an affiliated terrorist organization. S. Rep. No. 110-209, at 2-5 (2007). The TSP was not carried out under FISA or with the authorization of the FISC. The President's confirmation of the program in 2005 led Congress to "inquire vigorously" into the TSP and to "carefully review[] the impact of technological change on FISA collection to assess whether amendments to FISA should be enacted." *Id.* at 2.

The Director of National Intelligence ("DNI") and other government officials explained the need for this legislation in various appearances before Congress from 2006 to 2008. As the DNI explained, it was necessary to amend FISA because its definition of "electronic surveillance" was "tie[d] to a snapshot of outdated technology." *Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intelligence*, 110th Cong., 1st Sess. 19 (2007) ("May 1, 2007 FISA Modernization Hrg."), at 19. The DNI explained further that, since the creation of the definition three decades previously, "[c]ommunications technology ha[d] evolved in ways that have had unforeseen consequences under [the statute]." *Id.*

More specifically, the DNI explained that, whereas international communications were predominantly carried by radio when FISA was enacted, that was no longer true: "Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally by fiber optic cables" – and therefore qualify as wire communications under FISA. *Id.* Thus, many international communications that would have been generally excluded from FISA regulation in 1978, when they were carried by radio, were now potentially included, due merely to a change in technology rather than any intentional decision by Congress. *Id.*[15]

Further, the DNI stated, with respect to the collection of wire communications, FISA's "electronic surveillance" definition "places a premium on the location of the collection." May 1, 2007 FISA Modernization Hrg. 19; *see* 50 U.S.C. § 1801(f)(2). The DNI explained that technological advances had rendered this distinction outmoded as well: "Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart." May 1, 2007 FISA Modernization Hrg. 19. In this environment, regulating communications differently based on the location of collection arbitrarily limits the government's intelligence-gathering capabilities. As the Director of the NSA elaborated in an earlier hearing:

> [As a communication travels the global communications network,] NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, especially in today's telecommunication universe. Intercept of a particular communication ... is

[15] *Compare* 50 U.S.C. § 1801(f)(2) (defining wire communication as "electronic surveillance" if, *inter alia*, one party is in the United States) *with* 50 U.S.C. § 1801(f)(3) (defining radio communication as "electronic surveillance" only if the sender and all intended recipients are in the United States).

> always probabilistic, not deterministic. No coverage is guaranteed. We need to be able to use all the technological tools we have.

FISA for the 21st Century: Hearing before the S. Comm. on the Judiciary, 109th Cong., 2nd Sess. (2006) (statement of then-NSA Director General Michael V. Hayden).

Although FISA was originally crafted to accommodate the government's collection of foreign and international communications as those operations were commonly conducted in 1978, the government in 2008 faced a different communications technology environment and a different terrorist threat and needed greater flexibility than the statute's terms allowed.[16] The fix needed for this problem, as a Department of Justice official put it, was a "technology-neutral" framework for surveillance of foreign targets – focused not on "how a communication travels or where it is intercepted," but instead on "who is the subject of the surveillance, which really is the critical issue for civil liberties purposes." May 1, 2007 FISA Modernization Hrg. 46 (statement of Asst. Att'y Gen. Kenneth L. Wainstein).

That review initially led to the enactment in August 2007 of the Protect America Act ("PAA"), Pub. L. No. 110-55 (2007). Congress enacted the PAA in order to bring FISA "up to date with the changes in communications technology," while at the same time preserving "the privacy interests of persons in the United States" and addressing the "degraded capabilities in the face of a

---

[16] As the DNI testified:

> In today's threat environment, … FISA ... is not agile enough to handle the community's and the country's intelligence needs. Enacted nearly 30 years ago, it has not kept pace with 21st century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S. – that is foreign – p[ersons] located outside the United States … This clogs FISA process with matters that have little to do with protecting civil liberties or privacy of persons in the United States. Modernizing FISA would greatly improve that process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

May 1, 2007 FISA Modernization Hrg. 18.

heightened terrorist threat environment" that resulted from FISA's "requirement of a court order to collect foreign intelligence about foreign targets located overseas." S. Rep. No. 110-209, at 5-6. The PAA fulfilled these purposes by empowering the DNI and the Attorney General to jointly authorize "the acquisition of foreign intelligence information concerning persons reasonably believed to be located outside the United States." 50 U.S.C. § 1805b(a). To authorize such collection, the PAA required the DNI and the Attorney General to certify, *inter alia*, that there were reasonable procedures in place for determining that the acquisition concerned persons (whether U.S. persons or non-U.S. persons) reasonably believed to be located outside the United States ("targeting procedures"), there were minimization procedures in place that satisfied FISA's requirements for such procedures, and a significant purpose of the acquisition was to acquire foreign intelligence information. *See* 50 U.S.C. § 1805b(a)(1)-(5). The PAA also authorized the FISC to review the DNI and Attorney General's determination regarding the reasonableness of the targeting procedures. Finally, the PAA authorized private parties who had been directed by the government to assist in effectuating surveillance under the statute to challenge the legality of such a directive in the FISC, 50 U.S.C. § 1805b(h)(1)(A), and to appeal an adverse decision to the Foreign Intelligence Surveillance Court of Review ("FISA Court of Review"), *id.* § 1805b(i).[17] One private party brought such a challenge, and both the FISC and the FISA Court of Review upheld the PAA. *See In re Directives*, 551 F.3d 1004 (FISC Ct. Rev. 2008) (holding that surveillance authorized under the PAA fell within the foreign intelligence exception to the warrant requirement and was otherwise reasonable under the Fourth Amendment).

[17] The FISA Court of Review is composed of three United States District or Circuit Judges who are designated by the Chief Justice of the United States. *See* 50 U.S.C. § 1803(b).

4. Section 702 of the FISA Amendments Act

Due to a sunset provision, the PAA expired in February 2008. In July 2008, Congress enacted the FISA Amendments Act of 2008 ("FAA"), Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436.[18] The FAA provision at issue here, Section 702 of the FAA (50 U.S.C. § 1881a), "supplements pre-existing FISA authority by creating a new framework under which the government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013).[19] Section 702 provides that, "upon the issuance" of an order from the FISC, the Attorney General and DNI may jointly authorize the "targeting of persons[20] reasonably believed to be located outside the United States" for a period of up to one year to acquire "foreign intelligence information." 50 U.S.C. § 1881a(a).[21] In accordance with the statutory limitations discussed below, Section 702 only

---

[18] In 2012, Congress reauthorized the FAA for an additional five years. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631.

[19] The FAA enacted other amendments to FISA, including provisions not at issue in this case that govern the targeting of United States persons outside the United States. *See* 50 U.S.C. § 1881b.

[20] A "person" under Section 702 is defined the same way as under FISA Title I. 50 U.S.C. §§ 1801(m), 1881(a). "Person" under FISA, however, cannot include an entire geographic region or foreign country. *See* Privacy and Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* at 20-21 (July 2, 2014), available at www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf (hereafter "PCLOB Report"). The PCLOB is an independent agency within the Executive Branch established by the Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53, signed into law in August 2007. The PCLOB was tasked by a bipartisan group of U.S. Senators to investigate Section 702, among other NSA authorities, and issue an unclassified report. As part of its investigation, the PCLOB held public hearings and reviewed classified information provided by the Intelligence Community, some of which was declassified for use in the PCLOB report. *Id.* at 1-3.

[21] The Attorney General and DNI may authorize targeting to commence under Section 702 before the FISC issues its order if they determine that certain "exigent circumstances" exist. 50 U.S.C. § 1881a(a), (c)(2). If that determination is made, the Attorney General and DNI must, as soon as practicable (and within seven days), submit for FISC review their Section 702 certification,

authorizes the targeting of persons who are both non-U.S. persons and reasonably believed to be located overseas to acquire foreign intelligence information as defined by the statute.

Under Section 1881a(b), the authorized acquisition must comply with each of the following requirements, which are directed at preventing the intentional targeting of U.S. persons[22] or persons located within the United States (whether they are U.S. persons or non-U.S. persons), or collection of communications known at the time of acquisition to be purely domestic:

> (1) The authorized acquisition "may not intentionally target any person known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a(b)(1).
>
> (2) It may not intentionally target a person outside the United States "if the purpose . . . is to target a particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a(b)(2).
>
> (3) It "may not intentionally target a United States person reasonably believed to be located outside the United States." 50 U.S.C. § 1881a(b)(3).
>
> (4) It may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. 50 U.S.C. § 1881a(b)(4).
>
> (5) The acquisition must be "conducted in a manner consistent with the [F]ourth [A]mendment." 50 U.S.C. § 1881a(b)(5).

Section 702 does not require an individualized court order addressing each non-U.S. person to be targeted under its provisions. Section 702 instead permits the FISC to approve annual certifications by the Attorney General and DNI that authorize the acquisition of certain categories of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The categories of information being sought under a certification

---

including the targeting and minimization procedures used in the acquisition. 50 U.S.C. § 1881a(g)(1)(B); *see* 50 U.S.C. § 1881a(d), (e), (g)(2)(B).

[22] Section 702 incorporates the definition of "United States person" from Title I of FISA. 50 U.S.C. § 1801(i); 50 U.S.C. § 1881(a).

must meet the statutory definition of foreign intelligence information. Section 702 certifications have authorized acquisition of foreign intelligence information such as information concerning international terrorism and the acquisition of weapons of mass destruction. *See* PCLOB Report at 25 & n. 71 (citing public statements by the General Counsels of the DNI, NSA, and FBI).

a. The Government's Submission to the FISC

Section 702 requires the government to obtain the FISC's approval of (1) the government's certification regarding the proposed collection, and (2) the targeting and minimization procedures to be used in the acquisition. 50 U.S.C. § 1881a(a), (c)(1), (i)(2), (3); *see* 50 U.S.C. § 1881a(d), (e), (g)(2)(B). The certification must be made by the Attorney General and DNI and must attest that:

> (1) there are targeting procedures in place, that have been or will be submitted for approval by the FISC, that are reasonably designed to ensure that the acquisition is limited to targeting persons reasonably believed to be located outside the United States and to prevent the intentional acquisition of purely domestic communications;
>
> (2) the minimization procedures meet the definition of minimization procedures set forth in Titles I and III of FISA (50 U.S.C. §§ 1801(h), 1821(4)) and have been or will be submitted for approval by the FISC;
>
> (3) guidelines have been adopted by the Attorney General to ensure compliance with the aforementioned limitations set forth in Section 1881a(b) prohibiting, among other things, the targeting of United States persons;
>
> (4) the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment;
>
> (5) a significant purpose of the acquisition is to obtain foreign intelligence information;
>
> (6) the acquisition involves obtaining "foreign intelligence information from or with the assistance of an electronic communication service provider"; and

(7) the acquisition complies with the limitations in Section 1881a(b).[23]

50 U.S.C. § 1881a(g)(2)(A)(i) - (vii); *see* 50 U.S.C. §§ 1801(h), 1821(4), 1881a(b); *cf.* 50 U.S.C. §§ 1801(e), 1881(a) (defining "foreign intelligence information"). Such certifications are "not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under [section 1881a(a)] will be directed or conducted." 50 U.S.C. § 1881a(g)(4).[24]

[CLASSIFIED INFORMATION REDACTED]

b. The FISC's Order(s)

The FISC must review the certification, targeting and minimization procedures, and any amendments thereto. 50 U.S.C. § 1881a(i)(1) and (2). It may also require the government to submit additional information through court filings or witness testimony, including regarding the application of the targeting and minimization procedures or the operation and scope of the proposed Section 702 collection program. *See* FISC Rules of Procedure 5(c) (stating that FISC judges have the authority to order any party to a proceeding to supplement the record by "furnish[ing] any information that the Judge deems necessary") and 17 (permitting sworn testimony of witnesses at hearings); *e.g. [Caption Redacted]*, 2011 WL 10945618, at *2-5 (FISC Oct. 3, 2011) (describing additional government filings with, and testimony before, the FISC in connection with Section 702 certifications).

If the FISC determines that the certification contains all the required elements and concludes that the targeting and minimization procedures and Attorney General guidelines for compliance with the statutory limitations are "consistent with" both the Act and "the [F]ourth [A]mendment," the FISC will issue an order approving the certification and the use of the targeting

[23] [CLASSIFIED INFORMATION REDACTED]

[24] [CLASSIFIED INFORMATION REDACTED]

and minimization procedures. 50 U.S.C. § 1881a(i)(3)(A). If the FISC finds deficiencies in the certification or procedures, it must issue an order directing the government to, at the government's election and to the extent required by the court's order, correct any deficiency within 30 days, or cease or not begin implementation of the authorization. 50 U.S.C. § 1881a(i)(3)(B).

[CLASSIFIED INFORMATION REDACTED]

c. Implementation of Section 702 Authority

The government acquires communications pursuant to Section 702 through compelled assistance from electronic communications service providers. 50 U.S.C. § 1881a(h). The government identifies to these service providers specific communications facilities (also referred to as "selectors"), such as email addresses and telephone numbers, that the government has assessed, through the application of FISC-approved targeting procedures, are likely to be used by non-U.S. persons reasonably believed to be located overseas who possess, communicate, or are likely to receive a type of foreign intelligence information authorized for collection under a certification approved by the FISC. *See* NSA, *The National Security Agency:Missions Authorities, Oversight and Partnerships* at 4 (Aug. 9, 2013) available at https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf (describing the NSA's collection of foreign intelligence information under Section 702). Selectors may not be key words or the names of targeted individuals because such terms would not identify specific communications facilities. *See* NSA Director of Civil Liberties and Privacy Office Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, at 4 (Apr. 16, 2014), available at http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf (hereinafter "NSA DCLPOB Report"); PCLOB Report at 32-33.

Once a selector has been tasked for acquisition pursuant to a FISC-approved targeting procedure, acquisition against that selector is compelled through a directive served on a provider. There are two types of Section 702 acquisition: collection from service providers (referred to in the PCLOB Report as "PRISM" collection) and "upstream" collection. *See* PCLOB Report at 33. In "PRISM" collection, the government sends a selector to a service provider who is compelled by the directive to provide to the government communications sent either to or from that selector (known as "to/from" communications). *Id.* "Upstream" collection involves acquisitions conducted with the compelled assistance of the providers that control the telecommunications backbone within the United States over which communications transit. *Id.* at 35. It includes the collection of "to/from" communications, and may further collect communications that refer to the particular selector (for example, a targeted email address in the body of the email) (also known as "abouts" communications).[25] *Id.* at 37.

[CLASSIFIED INFORMATION REDACTED]

d. Targeting and Minimization Procedures

The government may conduct acquisitions under Section 702 only in accordance with specific targeting and minimization procedures that are subject to review and approval by the FISC. 50 U.S.C. § 1881a(c)(1)(A), (d), (e), and (i)(3)(A). Not only must the targeting procedures be reasonably designed to restrict acquisitions to the targeting of persons reasonably believed to be outside the United States and applied using compliance guidelines to ensure that the acquisitions do not intentionally target U.S. persons or persons located in the United States, 50 U.S.C. § 1881a(b), (d)(1) and (f)(1)(A), the minimization procedures also must be reasonably designed to minimize any acquisition of nonpublicly available information about unconsenting U.S. persons, and to minimize

[25] *See [Caption Redacted]*, 2011 WL 10945618 at *6, n.16 ("[A]ll 'about' communications are acquired by means of NSA's acquisition of Internet transactions through its upstream collection.").

the retention and prohibit the dissemination of any such information that might still be acquired, consistent with the need to obtain, produce, and disseminate foreign-intelligence information. 50 U.S.C. §§ 1801(h)(1), 1821(4)(A); *see* 50 U.S.C. § 1881a(e)(1).[26] The FISC, in turn, must substantively review the targeting and minimization procedures to ensure that they satisfy the statutory criteria and are consistent with the Fourth Amendment. 50 U.S.C. § 1881a(i)(2)(B), (C) and (3)(A).

The NSA, FBI, and CIA have separate sets of minimization procedures that govern each agency's retention and dissemination of information acquired through Section 702.[27] PCLOB Report at 51. Each set of minimization procedures takes into account the unique mission of the agency and the systems in which each agency stores and analyzes Section 702-acquired information.

[CLASSIFIED INFORMATION REDACTED]

i. Targeting Procedures

There are two agencies that conduct acquisitions under Section 702: the NSA and the FBI. Each agency conducts acquisitions pursuant to separate sets of targeting procedures. Other intelligence agencies can provide the NSA with "lead" information to initiate the collection from a selector. *See* PCLOB Report at 42.

Once the NSA identifies a potential person to target through tasking a selector, the targeting procedures require the NSA to assess whether the potential target is a non-U.S. person

---

[26] Minimization procedures may also "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. § 1801(h)(3). The definitions of minimization procedures in 50 U.S.C. §§ 1801(h)(4) and 1821(4)(D), which apply only to electronic surveillance approved pursuant to 50 U.S.C. § 1802(a) and physical searches approved pursuant to 50 U.S.C. § 1822(a), respectively, do not apply to acquisitions conducted under Section 702.

[27] The National Counterterrorism Center also is subject to minimization procedures, but its role in processing and minimizing Section 702 data is limited. *See* PCLOB Report at 51 n. 215.

reasonably believed to be located outside the United States, and whether the target possesses and/or is likely to communicate or receive foreign intelligence information authorized under an approved certification. *See id.* at 43. The determination regarding the location and non-U.S. person status is based on the totality of the circumstances. *Id.* If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting. *Id.* at 44. In making the foreign intelligence purpose determination, the NSA must identify the specific foreign power or foreign territory concerning which the foreign intelligence information is being sought. *Id.* at 45. The targeting procedures require documentation of the NSA's determinations. *Id.*

In addition, tasking requests by NSA analysts undergo an internal approval process prior to a selector being tasked for acquisition. *Id.* at 46. As discussed below, tasking requests may also be subject to additional review by external oversight teams with the Department and the Office of the DNI (hereinafter "ODNI"). *Id.*

The FBI's targeting procedures govern certain aspects of the collection of "to/from" communications, specifically requests for certain communications for selectors that have already been determined by the NSA to have met its targeting procedures. *Id.* at 47. Its targeting procedures are intended to "provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States." *See [Caption Redacted]*, 2011 WL 10945618, at *7 . The targeting procedures therefore require the FBI to both review the NSA's determinations regarding the non-U.S. person status and overseas location of the target, and review information available to the FBI. PCLOB Report at 47.

[CLASSIFIED INFORMATION REDACTED]

After tasking, the NSA targeting procedures impose additional requirements designed to ensure that the users of tasked selectors remain non-U.S. persons located outside the United States and that acquisition against the selector continues only insofar as the government assesses that the tasking is likely to acquire foreign intelligence information within one of the authorized Section 702 certifications. PCLOB Report at 48.

[CLASSIFIED INFORMATION REDACTED]

ii. *Minimization Procedures*

As noted above, Section 702 also requires the adoption of minimization procedures that comply with FISA's definition of such procedures. *See* 50 U.S.C. § 1881a(e)(1). FISA-compliant minimization procedures are, in pertinent part:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information . . . , shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

50 U.S.C. § 1801(h); *see also* 50 U.S.C. § 1821(4); 50 U.S.C. § 1801(e) (defining "foreign intelligence information"). All Section 702-acquired information is subject to the FISC-approved minimization procedures.

As a general matter, the minimization procedures of agencies that conduct Section 702 acquisitions (the NSA and FBI) contain provisions that minimize the acquisition of U.S. person information consistent with the authorized purpose of the collection. *See* PCLOB Report at 51. The minimization procedures for agencies who handle Section 702 collection (the NSA, CIA and FBI) also contain limitations on the use and dissemination of U.S. person information acquired through Section 702 acquisitions. *Id.* at 53, 64. For example, the minimization procedures permit the dissemination of U.S. person information only if any information that could identify the U.S. person is deleted, absent certain specific circumstances. Such circumstances may include where the U.S. person has consented to the dissemination, the specific information about the U.S. person is already publicly available, the U.S. person's identity is necessary to understand foreign intelligence information, or the communication contains evidence of a crime and is being disseminated to law enforcement authorities. *Id.* at 64-65.

[CLASSIFIED INFORMATION REDACTED]

e. Oversight

Section 702 requires that the Attorney General and DNI periodically assess the government's compliance with both the targeting and minimization procedures and with relevant compliance guidelines, and that they submit those assessments both to the FISC and to Congressional oversight committees. 50 U.S.C. § 1881a(l). In addition, not less often than once every six months, the Attorney General must keep the relevant Congressional oversight committees "fully inform[ed]" concerning the implementation of Section 702. 50 U.S.C. § 1881f(a) and (b)(1); *see also Clapper*, 133 S. Ct. at 1144 ("Surveillance under [Section 702] is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment."). Such committees include the Senate Select Committee on Intelligence, Senate

Committee on the Judiciary, House Permanent Select Committee on Intelligence, and House Judiciary Committee. *See* PCLOB Report at 69.

The government's use of the Section 702 authorities is also subject to internal oversight by various entities within each agency that has a role in the acquisition, retention, or dissemination of Section 702 information. *See id.* at 66-68. Moreover, incidents of non-compliance with the targeting or minimization procedures that are identified by any internal compliance efforts, or that are otherwise self-identified by the agencies, must be reported to the Department of Justice and ODNI. *Id.* at 68.

In addition, the FISC Rules of Procedure require the government to notify the FISC whenever the government discovers a material misstatement or omission in a prior filing with the court, including with respect to Section 702 certifications. *See* FISC R. P. 17; *e.g. [Caption Redacted]*, 2011 WL 10945618, at *2. Rule 13(b) of the Rules of Procedures for the FISC requires the government to report, in writing, all instances of non-compliance. FISC R. P. 13b(1). The government reports Section 702 compliance incidents to the FISC via individual notices and quarterly reports.[28, 29] *See* NSA DCLPOB Report at 3. The FISC has noted that it considers implementation problems when evaluating the sufficiency of the government's certification. Specifically, the FISC "has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired" and that "[s]ubstantial implementation problems can, notwithstanding the government's intent, speak to whether the applicable targeting procedures are 'reasonably designed' to acquire only the

[28] Depending on the type or severity of compliance incidents, the NSA also may promptly notify the relevant Congressional intelligence committees of an individual compliance matter.

[29] [CLASSIFIED INFORMATION REDACTED]

communications of non-U.S. persons outside of the United States." *See [Caption Redacted]*, 2011 WL 10945618, at *9.

f. District Court Review of FISC Orders and Section 702 Collection

Both FISA and the FAA authorize the use in a criminal prosecution of information obtained or derived from FISA-authorized electronic surveillance or physical searches or Section 702 collection, provided that advance authorization is obtained from the Attorney General and proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used. *See* 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e), and 1881e(a). 50 U.S.C. § 1881e(a) provides that information acquired pursuant to Section 702 is "deemed to be" information acquired pursuant to Title I of FISA for, among other things, the purposes of the applicability of the statutory notice requirement and the suppression and discovery provisions of Section 1806.

Under Section 1806(c), the government's notice obligation applies only if the government "intends to enter into evidence or otherwise use or disclose" (2) against an "aggrieved person" (3) in a "trial, hearing or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) an "electronic surveillance [or physical search] of that aggrieved person." 50 U.S.C. § 1806(c); *see* 50 U.S.C. § 1825(d).[30] Where all five criteria are met, the government will notify the defense and the Court (or other authority) in which the information is to be disclosed or used that the government intends to use or disclose such information. The "aggrieved" defendant may then challenge the use of that information in district court on two grounds: (1) that the

[30] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2).

information was unlawfully acquired; or (2) that the acquisition was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e) and (f), 1881e(a).[31] In addition, FISA contemplates that a defendant may file, as Hasbajrami has done, a motion or request under any other statute or rule of the United States to discover or obtain applications or orders or other materials relating to electronic surveillance or physical searches, *i.e.,* the FISA materials, 50 U.S.C. §§ 1806(f), 1825(g).

When a defendant moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 1825(f) or Section 702 information, or seeks to discover the FISA or Section 702 materials under some other statute or rule, the district court must determine whether the collection of the aggrieved person was lawfully authorized and conducted. *See* 50 U.S.C. § 1806(f). With respect to such motions relating to FISA, the motion or request is evaluated using FISA's probable cause standard, which is discussed below, and not the probable cause standard applicable to criminal warrants. *See, e.g., United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011); *United States v. Duka*, 671 F.3d 329, 336-37 (3d Cir. 2011) (rejecting appellant's challenge to FISA's probable cause standard because it does not require any indication that a crime has been committed); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987).

In assessing the legality of the collection at issue, the district court, "shall, notwithstanding any other law, if the Attorney General files [as he has filed in this proceeding] an affidavit [or declaration] under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other

[31] Separately, any electronic communications service provider the government directs to assist in Section 702 surveillance may challenge the lawfulness of that directive in the FISC. 50 U.S.C. § 1881a(h)(4) and (6); *see also In re Directives*, 551 F.3d at 1004 (adjudicating Fourth Amendment challenge brought by electronic communications service provider to directive issued under the PAA).

materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g). On the filing of the Attorney General's affidavit or declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]. *Id.* If the district court is able to make an accurate determination of the legality of the surveillance or search based on its *in camera*, *ex parte* review of the materials submitted by the United States, then the court may not order disclosure of any of the FISA or FAA materials to the defense, unless otherwise required by due process. *See id.*

II. THE DEFENDANT'S CONSTITUTIONAL ARGUMENTS LACK MERIT

The defendant moves for suppression of evidence derived from the acquisition of foreign intelligence information under Section 702 on the ground that Section 702 is unconstitutional. (Def. Mot. 5-31). For the reasons set forth below, the defendant's motion should be denied.

A. THE ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION UNDER SECTION 702 IS LAWFUL UNDER THE FOURTH AMENDMENT

The collection at issue in this case, pursuant to Section 702 and the applicable certifications and targeting and minimization procedures, was consistent with the Fourth Amendment.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" and that "no Warrants shall issue, but upon probable cause." "[A]lthough 'both the

concept of probable cause and the requirement of a warrant bear on the reasonableness of a search,'" *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (citation omitted), "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." *Nat'l Treas. Employees Union v. Von Raab*, 489 U.S. 656, 665 (1989). The "touchstone" of a Fourth Amendment analysis "is always 'the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security.'" *Pennsylvania v. Mimms*, 434 U.S. 106, 108-09 (1977) (per curiam) (quoting *Terry v. Ohio*, 392 U.S. 1, 19 (1968)).

The Section 702-authorized collection at issue in this case, which was conducted pursuant to court-approved procedures reasonably designed to target non-U.S. persons located outside the United States, was reasonable under the Fourth Amendment. First, the Fourth Amendment generally does not apply to non-U.S. persons abroad, and the fact that collection targeting such persons also incidentally collects communications of U.S. persons does not trigger a warrant requirement or render the collection constitutionally unreasonable. Second, surveillance conducted under Section 702 falls within the well-recognized "foreign intelligence exception" to the warrant requirement because (1) the government's purpose – protecting against terrorist attacks and other external threats – extends "beyond routine law enforcement," and (2) "insisting upon a warrant would materially interfere with the accomplishment of that purpose." *In re Directives*, 551 F.3d at 1010-11.

Given the inapplicability of the warrant requirement, the challenged collection need only meet the Fourth Amendment's general reasonableness standard. That standard is satisfied here. The government has interests of the utmost importance in obtaining foreign intelligence information under Section 702 to protect national security. In contrast, the privacy interests of U.S. persons in

international communications are significantly diminished when those communications have been transmitted to or obtained from non-U.S. persons located outside the United States.

Finally, the privacy interests of U.S. persons whose communications are incidentally collected are amply protected by stringent safeguards the government employs in implementing the collection. Those safeguards include (1) certifications by Executive Branch officials concerning the permissible foreign intelligence purposes of the collection; (2) court-approved targeting procedures designed to ensure that only non-U.S. persons abroad are targeted; (3) court-approved minimization procedures to protect the privacy of U.S. persons whose communications are incidentally acquired; (4) the requirement of a significant purpose to obtain foreign intelligence information; (5) extensive oversight within the Executive Branch, as well as by Congress and the FISC; and (6) a prior judicial finding that the targeting and minimization procedures are consistent with the Fourth Amendment.

In light of these and other safeguards, the FISC has repeatedly concluded that acquisition of foreign intelligence information under Section 702 and the applicable targeting and minimization procedures is constitutionally reasonable. The only other court that has decided on the merits a motion to suppress Section 702-derived evidence has upheld the constitutionality of Section 702 and, in doing so, the court rejected many of the same arguments that the defendant raises here. *See United States v. Mohamud*, 3:10-CR-00475-KI-1, 2014 WL 2866749 (D. Or. June 24, 2014). This Court should reach the same conclusion.

1. There is No Judicial Warrant Requirement Applicable to Foreign Intelligence Collection Targeted at Foreign Persons Abroad

Defendant's principal contention (Def. Mot. 5-31) is that, because he is a U.S. person who at the relevant time was located in the United States, collection of his communications under Section 702 must satisfy the requirements of the Fourth Amendment's Warrants Clause. Defendant's contention ignores the fact that Section 702 only authorizes collection of foreign

intelligence information by targeting non-U.S. persons outside the United States, and he cites no precedent indicating that such surveillance requires a warrant.[32] The fact that communications of U.S. persons such as the defendant might incidentally be collected pursuant to such surveillance does not alter the principle that a judicial warrant is not required for foreign intelligence surveillance targeting foreign persons abroad pursuant to Section 702.

a. The Fourth Amendment Generally Does Not Apply to Non–U.S. Persons Abroad

The Supreme Court has held that the Fourth Amendment does not "apply to activities of the United States directed against aliens in foreign territory." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990); *see also id.* at 271 (noting that only persons who "have come within the territory of the United States and developed substantial connections" to the country have Fourth Amendment rights). Based on the Fourth Amendment's text, drafting history, and post-ratification history, *id.* at 265-67, as well as its own precedents, *id.* at 268-71, the Supreme Court concluded that the Fourth Amendment was not intended "to restrain the actions of the Federal Government against aliens outside of the United States territory," *Id.* at 266. "If there are to be restrictions on searches and seizures which occur incident to such American action," the Court explained, "they must be imposed by the political branches through diplomatic understanding, treaty, or legislation." *Id.* at 275. Because the Fourth Amendment generally does not protect non-U.S. persons outside the United States, at least where such persons lack "substantial connections" to this country, the Fourth Amendment *a fortiori* does not prevent the government from subjecting them to surveillance without a warrant.

Intelligence collection under Section 702 targets non-U.S. persons located outside the United States. Accordingly, under *Verdugo-Urquidez*, the Fourth Amendment generally is

[32] [CLASSIFIED INFORMATION REDACTED]

inapplicable to persons who are targeted for collection in accordance with the requirements of the statute.[33] For that reason, to the extent the defendant attempts a facial challenge to Section 702 (*see* Def. Mot. 13), the challenge fails, because the statute is constitutional in its application to persons unprotected by the Fourth Amendment. *See United States v. Salerno*, 481 U.S. 739, 745 (1987) (noting that, outside of the First Amendment context, a statute is facially invalid only if it is unconstitutional in all of its possible applications).[34]

b. Incidental Collection of Communications of U.S. Persons Pursuant to Intelligence Collection Lawfully Targeting Non-U.S. Persons Located Outside the United States Does Not Trigger A Warrant Requirement

The statute does not permit U.S. persons or non-U.S. persons located in the United States to be intentionally targeted under Section 702. To the extent that the government collects communications of U.S. persons *incidentally* under Section 702 in the course of intelligence

---

[33] The head of each element of the intelligence community must report annually to the FISC concerning, *inter alia*, how many persons the element targeted under Section 702 (based on the belief that the persons were located outside the United States) who were later determined to be located inside the United States. *See* 50 U.S.C. § 1881a(1)(3)(A)(iii).

[34] The question whether a statute may ever be facially invalid under the Fourth Amendment is currently pending before the Supreme Court. *See City of Los Angeles v. Patel*, No. 13-1175 (cert. granted Oct. 20, 2014). However, even if the Court holds that facial Fourth Amendment challenges are permitted and even if the Court applies the more lenient "overbreadth" standard to Fourth Amendment facial challenges (rather than the *Salerno* standard in which the challenger must establish that no set of circumstances exists under which the law would be valid), any facial challenge to Section 702 would fail in light of the statute's "plainly legitimate sweep" in its application to communications of non-U.S. persons abroad who lack Fourth Amendment rights. *See Washington v. Glucksberg*, 521 U.S. 702, 740 n.7 (1997) (noting that even "the most lenient standard that [the Court has] applied requires the challenger to establish that the invalid applications of a statute must not only be real, but substantial as well, judged in relation to the statute's plainly legitimate sweep"). Accordingly, this Court's review should be limited to the constitutionality of the statute as applied to the acquisition of the information challenged in this case. *See United States v. Duggan*, 743 F.2d 59, 71 (2d Cir. 1984) (rejecting defendant's attempt to challenge surveillance based on arguments that FISA was "impermissibly broad" because the arguments "ha[d] no application to the case at hand"); *United States v. Mohamud*, 3:10-CR-00475, 2014 WL 2866749, at *13-*14 (D. Or. June 24, 2014) (limiting criminal defendant's Fourth Amendment challenge to Section 702 to an "as-applied" challenge).

collection targeted at one or more non-U.S. persons outside the United States, "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful." *In re Directives*, 551 F.3d at 1015; *United States v. Kahn*, 415 U.S. 143, 156-57 (1974) (upholding interception of communications of a woman that were incidentally collected pursuant to a criminal wiretap order targeting her husband); *see also United States v. White*, 401 U.S. 745, 751-53 (1971) (holding that a conversation recorded with the consent of one participant did not violate another participant's Fourth Amendment rights); *United States v. Figueroa*, 757 F.2d 466, 472-73 (2d Cir. 1985) (rejecting challenge to Title III on the ground that it allows interception of conversations of unknown third parties); *United States v. Tortorello*, 480 F.2d 764, 775 (2d Cir. 1973) (when relevant authority is established for surveilling one participant in a conversation, "the statements of other participants may be intercepted if pertinent to the investigation"); *United States v. Butenko*, 494 F.2d 593, 608 (3d Cir. 1974) (upholding the constitutionality of warrantless surveillance for foreign intelligence purposes even though "conversations . . . of American citizens[] will be overheard"); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.").

Under these principles, incidental capture of a U.S. person's communications during surveillance that lawfully targets non-U.S. persons abroad does not imply that a judicial warrant or other individualized court order is required for such surveillance to be reasonable under the Fourth Amendment. *See Bin Laden*, 126 F. Supp. 2d at 281 (noting that "the combination of *Verdugo-Urquidez* and the incidental interception cases" would permit surveillance that collects a U.S. person's communications as an incident to warrantless surveillance targeting a non-U.S. person abroad, so long as the U.S. person is not a "known and contemplated" surveillance target). Thus,

surveillance of non-U.S. persons outside the United States pursuant to Section 702, even without a warrant or probable cause, is not rendered unlawful if the surveillance incidentally captures the communications of non-targeted persons in the United States. *See Mohamud*, 2014 WL 2866749, at *15 (holding that, as a "general rule," the "incidental collection of [U.S. person] communications with a [foreign] target" pursuant to Section 702 is "lawful," and rejecting the claim that the potential for incidental collection of large numbers of U.S. person communications warrants an exception to that rule). This conclusion is particularly appropriate here because the privacy interests of persons whose communications are incidentally collected are further protected by minimization procedures, as described *supra*. *See In re Directives*, 551 F.3d at 1016 (noting that the minimization procedures under the PAA "serve . . . as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons").

The defendant and *amici* contend (Def. Mot. 12; Br. 13-16) that collection of U.S. persons' communications during surveillance targeting non-U.S. persons outside the United States is not properly considered "incidental" because the government knows that, inevitably, some of the foreign targets will communicate with U.S. persons, and the minimization procedures permit the government in certain circumstances to retain those communications. However, the same is true of Title I FISA electronic surveillance or law enforcement wiretaps pursuant to Title III, in which, inevitably, the government collects communications of third parties and the minimization procedures permit retention of those communications in certain circumstances. *Amici* further rely (Br. 13 & n.24) on statements in the PAA legislative history indicating the government has a foreign intelligence interest in communications that the foreign targets may have with persons located in the United States. However, the fact that one purpose of surveillance that lawfully targets a foreign person located outside the United States may also be to discover whether the foreign targets are in

contact with individuals in the United States does not mean that collection of such communications requires a separate warrant or is constitutionally unreasonable. Again, *amici*'s reasoning applies equally to traditional FISA electronic surveillance or ordinary law enforcement wiretaps under Title III, where frequently one of the purposes of the surveillance is to discover the identities, locations, and activities of previously unknown third parties who may be, for example, involved in a terrorist network targeted by traditional FISA electronic surveillance or co-conspirators of a drug kingpin targeted under Title III. In those circumstances, collection of communications of the non-targeted third parties is properly considered "incidental" to surveillance that is lawful as to the target and no separate warrant as to those third parties is required. The same is true of Section 702 collection. *In re Directives*, 551 F.3d at 1015.

Application of a warrant requirement to incidental interception of U.S. person communications during surveillance targeting non-U.S. persons abroad for foreign intelligence purposes not only would be contrary to case law but also would be impracticable and inconsistent with decades of foreign-intelligence collection practice. *See In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 169 (2d Cir. 2008) (holding that the warrant requirement does not apply to searches or surveillance of U.S. citizens that occur outside the United States because the original purpose of the Fourth Amendment "was to restrict searches and seizures which might be conducted by the United States in domestic matters"); *United States v. Stokes*, 726 F.3d 880, 893 (7th Cir. 2013) (rejecting warrant requirement for extraterritorial searches targeting United States persons and holding such searches "are subject only to the Fourth Amendment's requirement of reasonableness").[35] Before initiating surveillance of a foreign target, the government cannot know

[35] While the defendant cites cases recognizing a warrant requirement for electronic surveillance in the domestic context (*See, e.g.*, Def. Mot. 21), he does not point to any authorities indicating that

the identities of all those with whom the target will communicate in the future, and there will generally be at least some possibility that the target will communicate with a U.S. person. *See Bin Laden*, 126 F. Supp. 2d at 280 ("[T]he government is often not in a position of omniscience regarding who or what a particular surveillance will record."). Thus, imposition of a warrant requirement for any incidental interception of communications of U.S. persons would effectively require a warrant for all foreign intelligence collection, even though the foreign targets lack Fourth Amendment rights and their communications often involve only other foreigners. Such a rule would unduly restrict the government's intelligence collection against foreign targets and degrade its ability to protect against foreign threats. *See Warrantless Surveillance and The Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II) Hearing Before the H. Judiciary Comm.*, 110th Cong., 1st Sess. 8 (2007) (statement of Rep. Forbes) ("To require a court order for every instance in which a foreign target communicates with someone inside the United States is to require a court order for every foreign target, and requiring this would reverse 30 years of established intelligence gathering . . . The intelligence community cannot possibly know ahead of time who these terrorists will talk to. It needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a person inside the United States.").

c. The Location of the Search Does Not Trigger a Warrant Requirement

Verdugo-Urquidez involved a physical search that was conducted overseas, while collection under Section 702 takes place within the United States. In the context of electronic communications, however, the fact that the communications of a non-U.S. person outside the United States may be collected from within the United States is not the kind of "significant voluntary

---

foreign intelligence surveillance targeting non-United States persons outside the United States must be subject to the warrant procedure.

connection with the United States" that brings that person within the protection of the Fourth Amendment under *Verdugo-Urquidez*. 494 U.S. at 271-72. Otherwise, any foreign person abroad seeking to evade United States surveillance, including al Qaeda terrorists, could claim the protections of the Fourth Amendment merely due to this type of insignificant connection to the United States. That result would be plainly contrary to the Supreme Court"s statements in *Verdugo-Urquidez* that the Fourth Amendment was not originally intended to protect "aliens outside of the United States territory." *Id.* at 266-67. Moreover, when the government collects the communications of a non-U.S. person located abroad, whether the collection takes place in the United States or abroad makes no difference to the person's privacy interests and should not affect the constitutional analysis. When it comes to the content of communications, "the Fourth Amendment protects people, not places." *United States v. Yonn*, 702 F.2d 1341, 1347 (11th Cir. 1983) (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). Accordingly, there is no "constitutional distinction which depends upon the location of the recording apparatus." *Id.*

2. The Foreign Intelligence Exception Applies

Even assuming, *arguendo*, that incidental collection of communications of U.S. persons under Section 702 is subject to the same constitutional scrutiny as foreign intelligence collection targeting such persons, *cf. [Caption Redacted]*, 2011 WL 10945618, at *26 (noting that "[t]here surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable"), the Fourth Amendment does not require a warrant here because such surveillance falls within the well-recognized foreign intelligence exception.

a. The "Special Needs" Doctrine

The touchstone of the Fourth Amendment is reasonableness, which is assessed by balancing the degree to which a search is needed to promote legitimate governmental interests

against the search's intrusion on a person's privacy interests. *See United States v. Knights*, 534 U.S. 112, 118-19 (2001). In certain contexts, a search or surveillance is impermissible without a warrant or other individualized court order. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995) ("Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant."). But that procedure is by no means inflexibly required. *Maryland v. King*, 133 S. Ct. 1958, 1969 (2013) (The Fourth Amendment "imposes no irreducible requirement" of individualized suspicion.); *see, e.g.*, *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004) (The government has "plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant.").

The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable," *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987), such as where the governmental need is especially compelling or especially likely to be frustrated by a warrant requirement, where expectations of privacy are diminished, and where alternative safeguards restrain the government within reasonable limits. *See King*, 133 S. Ct. at 1969; *see also*, *e.g.*, *Griffin*, 483 U.S. at 873-74, (upholding warrantless search of probationer's home); *Vernonia Sch. Dist.*, 515 U.S. at 653 (upholding warrantless drug testing of student-athletes by public school district); *Samson v. California*, 547 U.S. 843, 847 (2006) (upholding suspicionless searches of parolees). In evaluating whether the "special needs" doctrine applies, the Supreme Court has distinguished between searches designed to uncover evidence "of ordinary criminal wrongdoing" and those motivated "at [a] programmatic level" by other governmental objectives. *City of Indianapolis v. Edmond*, 531 U.S. 32, 37-40, 48 (2000) (reviewing cases).

The "special needs" doctrine applies where special government interests beyond the normal need for law enforcement make the warrant and probable-cause requirement impracticable, and in such cases the court "employ[s] a balancing test that weigh[s] the intrusion on the individual's interest in privacy against the 'special needs' that supported the program." *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001). Accordingly, the Supreme Court has permitted, *inter alia*, warrantless stops of motorists at roadblocks for the purpose of securing borders, *see United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), warrantless searches of the homes of probationers to ensure compliance with probation conditions, *see Griffin*, 483 U.S. at 872, and warrantless searches of public school students to enforce school rules, *see T.L.O.*, 469 U.S. at 340. The Second Circuit has upheld physical searches conducted for the "programmatic purpose" of protecting the nation against terrorist threats on the ground that such searches involve special government interests beyond the normal need for law enforcement. *See Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (upholding warrantless searches of ferry passengers because "preventing or deterring large-scale terrorist attacks present problems that are distinct from standard law enforcement needs"); *MacWade v. Kelly*, 460 F.3d 260, 271 (2d Cir. 2006) (recognizing, in upholding warrantless searches of subway passengers, that "preventing a terrorist from bombing the subways constitutes a special need that is distinct from ordinary *post hoc* criminal investigation").

b. The Foreign Intelligence Exception

Several courts of appeals – including the FISA Court of Review – have held, by analogy to the "special needs" doctrine, that the government's "special need" for foreign intelligence information justifies an exception to the warrant requirement. *See, e.g., Duka*, 671 F.3d at 341 ("[C]ourts [that have considered the question] almost uniformly have concluded that the important national interest in foreign intelligence gathering justifies electronic surveillance without prior

judicial review, creating a sort of 'foreign intelligence exception' to the Fourth Amendment's warrant requirement."); *In re Directives*, 551 F.3d at 1010-11 (recognizing "a foreign intelligence exception" to the warrant requirement); *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."); *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-13 (4th Cir. 1980) (upholding warrantless foreign intelligence surveillance authorized by the Attorney General); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement."); *Butenko*, 494 F.2d at 605; *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973);[36] *but see Zweibon v. Mitchell*, 516 F.2d 594, 618-20 (D.C. Cir. 1975) (en banc) (plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation).[37] These decisions have found that foreign intelligence collection justifies an exception because the "programmatic purpose" of obtaining foreign intelligence information goes "beyond any garden-variety law enforcement objective," and "requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011.

---

[36] Except for *In re Directives*, these cases involved collection of foreign intelligence information from persons inside the United States. Their reasoning applies *a fortiori* to the Section 702 acquisition in this case, which targeted non-United States person(s) reasonably believed to be outside the United States. *Cf. In re Terrorist Bombings*, 552 F.3d at 172 (declining to analyze foreign search of a U.S. person under the foreign intelligence exception, because the warrant requirement is "inapplicable to foreign searches" regardless of whether the search is conducted for foreign intelligence purposes).

[37] The plurality in *Zweibon* specifically noted that the surveillance at issue targeted a domestic organization and suggested that its conclusion might be different if a foreign power were targeted. *See* 516 F.2d at 651.

The defendant relies (Def. Mot. 14-18) on the Supreme Court's decision in *United States v. U.S. District Court (Keith)*, 407 U.S. 297 (1972). This reliance is misplaced, as the Court in *Keith* expressly reserved the issue of a warrant requirement for foreign intelligence collection. As the FISA Court of Review recognized in *In re Sealed Case*, the Supreme Court explained in *Keith* that "the focus of security surveillance 'may be less precise than that directed against more conventional types of crime' even in the area of *domestic* threats to national security." 310 F.3d at 738 (emphasis in original); *see also Clapper*, 133 S. Ct. at 1143 (noting that *Keith* "implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible"). The same rationale "applies *a fortiori* to foreign threats," a fact that Congress necessarily recognized in enacting FISA. *In re Sealed Case*, 310 F.3d at 738; *see also Truong*, 629 F.2d at 913 ("For several reasons, the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate' the President in carrying out his foreign affairs responsibilities."). In addition, unlike the intelligence collection at issue here, the surveillance in *Keith* was conducted not only without a warrant but without any judicial or congressional oversight of any kind. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-37 (1952) (Jackson, J. concurring) ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum."). Courts that have addressed the issue of whether foreign intelligence collection is subject to a warrant requirement have expressly distinguished *Keith* in holding that it is not. *In re Directives*, 551 F.3d at 1010; *In re Sealed Case*, 310 F.3d at 744; *Truong*, 629 F.2d at 913; *Butenko*, 494 F.2d at 602 n.32; *Brown*, 484 F.2d at 425.

In sum, courts have generally recognized, by analogy to the "special needs" doctrine, that a foreign intelligence exception to the warrant requirement exists. As the FISC has held, and

for the reasons set forth below, that exception applies to acquisitions under Section 702. *[Caption Redacted]*, 2011 WL 10945618, at *24 ("The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the 'foreign intelligence exception' to the warrant requirement of the Fourth Amendment."); *Mohamud*, 2014 WL 2866749, at *18 (holding that "the foreign intelligence exception applies" to Section 702 collection and therefore "no warrant is required").

c. The Government's Purpose in Section 702 Collection Goes Beyond Ordinary Crime Control

First, it is clear that the government's programmatic purpose in obtaining the information pursuant to Section 702 goes beyond routine law enforcement. *See In re Sealed Case*, 310 F.3d at 717 (holding that the government's "programmatic purpose" in obtaining foreign intelligence information is "to protect the nation against terrorist and espionage threats directed by foreign powers" – "a special need" that fundamentally differs from "ordinary crime control."); *see also Cassidy*, 471 F.3d at 82; *MacWade*, 460 F.3d at 271. Acquisitions under Section 702 must be conducted with a "significant purpose" to "obtain foreign intelligence information." 50 U.S.C. § 1881a(g)(2)(v); s*ee also Duka*, 671 F.3d at 343-45 (surveillance based on the "significant purpose" requirement is reasonable under the Fourth Amendment). As the FISA Court of Review found in the context of the PAA, the "stated purpose" of the collection "centers on garnering foreign intelligence," and "[t]here is no indication that the collections of information are primarily related to ordinary criminal-law enforcement purposes." The same is true of collection authorized under Section 702.[38] *Mohamud*, 2014 WL 2866749, at *18.

[38] [CLASSIFIED INFORMATION REDACTED]

d. A Warrant or Probable Cause Requirement Would Be Impracticable

Second, as the FISA Court of Review found with respect to the FAA's predecessor statute, "there is a high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011; *see also Truong*, 629 F.2d at 913 (noting that "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy" and, therefore, "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations").[39] Changes in technology and the manner of collecting foreign intelligence information, as well as the shifting threat and communications methods employed by transnational terrorist groups, make it impracticable for the government to obtain traditional warrants or FISC orders for the acquisitions currently authorized under Section 702. Indeed, Congress enacted the FAA in part because the burden of preparing individualized FISA applications for intelligence collection targeting non-U.S. persons outside the United States was harming the government's ability to collect foreign intelligence information from targets overseas. *See* 154 Cong. Rec. S6097, S6122 (June 25, 2008) (statement of Sen. Chambliss) ("[T]he [FAA] will fill the gaps identified by our intelligence officials and provide them with the tools and flexibility they need to collect intelligence from targets overseas.").

When the government has reason to believe that a non-U.S. person overseas is connected to international terrorist activities but the government lacks sufficient evidence to establish probable cause that the target is an agent of a foreign power, a warrant requirement could

[39] [CLASSIFIED INFORMATION REDACTED]

prevent the government from obtaining significant information. Even in circumstances where the government succeeded in eventually gathering enough information to establish probable cause under FISA, the need to develop such information and obtain approval of the FISC could result in delays that would hinder the government's ability to monitor fast-moving threats. *See In re Directives*, 551 F.3d at 1011-12 (Because of the government's "need for speed, stealth, and secrecy" in this context, "[c]ompulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government's ability to collect information in a timely manner"); PCLOB Report at 104-06 (recognizing value in the "flexibility" that Section 702 "enables" by "allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision"); *cf. Verdugo-Urquidez*, 494 U.S. at 273-74 ("Application of the Fourth Amendment" to aliens abroad could "significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest."); *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 623 (1989) (upholding warrantless search in part because "the delay necessary to procure a warrant . . . may result in the destruction of valuable evidence").

In short, a warrant requirement would significantly undermine the government's ability to obtain foreign intelligence information vital to the Nation's security. *See Bin Laden*, 126 F. Supp. 2d at 273 ("[T]he imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden" on the government's ability to obtain foreign intelligence information). That would be a particularly unnecessary result because Section 702 collection may not intentionally target persons protected by the Fourth Amendment, *see* 50 U.S.C. § 1881a(b), and the law contains robust safeguards that protect the interests of such persons whose communications might be incidentally collected. *See United States v. Abu-Jihaad*, 630 F.3d 102, 121-22 (2d Cir.

2010) ("[T]he Constitution's warrant requirement is flexible, so that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations at issue.") (internal quotation marks and citation omitted).

e. A Warrant Requirement Would Inappropriately Interfere with Executive Branch Discretion in the Collection of Foreign Intelligence

The Fourth Amendment's warrant requirement is based in part on the interest in "interpos[ing] a judicial officer between the zealous police officer ferreting out crime and the subject of the search." *In re Terrorist Bombings*, 552 F.3d at 170 n.7. But that concern is considerably diminished in this context because of "the acknowledged wide discretion afforded the executive branch in foreign affairs." *Id.*; *see Truong*, 629 F.2d at 914 ("[T]he executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs."). For that reason, the Fourth Amendment does not require that courts interpose themselves in the Executive Branch's collection of foreign intelligence beyond the procedures provided for by Congress.

f. Section 702 Collection Falls Within the Scope of the Foreign Intelligence Exception

Amici contend (Br. 16-18) that the foreign intelligence exception is limited to circumstances where: (1) the surveillance was directed at a specific foreign agent or foreign power; and (2) the surveillance was personally approved by the President or Attorney General. This argument should be rejected.

While the court in *In re Directives* recognized the requirement that surveillance *targeting U.S. persons* under the PAA must be directed at a foreign power or its agent, the court did not hold or suggest that such a requirement is necessary for surveillance targeting *non-U.S. persons* abroad in order to fall within the foreign intelligence exception. *See In re Directives*, 551 F.3d at

1012. Indeed, the court specifically upheld the constitutionality of surveillance targeting non-U.S. persons abroad that incidentally collected U.S. person communications, even though the PAA did *not* require surveillance targeting non-U.S. persons abroad to be directed at a specific foreign power or its agent.[40] *See id.* at 1015. And, for the reasons explained above, such a requirement would seriously undermine the government's ability to obtain foreign intelligence information in this context and, in any event, would be unnecessary since the targets of the surveillance are persons unprotected by the Fourth Amendment.[41]

As for the second purported limitation *amici* invoke, it is true that the Attorney General does not personally approve each individual acquisition under Section 702. However, the Attorney General and Director of National Intelligence play a significant role in establishing and authorizing the certification and procedures that govern the acquisition. *See* 50 U.S.C. 1881a(a) (collection under Section 702 must be jointly authorized by the Attorney General and Director of National Intelligence). In addition, unlike the unilateral executive branch surveillance in *Truong*, Section 702 collection is governed by stringent, court-approved procedural safeguards and extensive oversight by the FISC and by Congress. Those requirements provide sufficient authorization and oversight, by all three branches of government, for purposes of the foreign intelligence exception.

3. The Government's Collection of Foreign Intelligence Information Pursuant to Section 702 is Constitutional Under the Fourth Amendment's General Reasonableness Test

As explained above, incidental collection of communications of U.S. persons and non-U.S. persons located in the United States during an otherwise lawful collection does not render

---

[40] *Amici*'s reliance on *Duka, In re Sealed Case*, and *Bin Laden* is equally unavailing because those cases addressed traditional FISA collection or collection targeting a U.S. person located overseas, not collection targeting *non-U.S. persons* located overseas.

[41] [CLASSIFIED INFORMATION REDACTED]

the collection constitutionally unreasonable. *See* Part II.A. That principle applies here because the collection lawfully targeted non-U.S. persons outside the United States for foreign intelligence purposes. Moreover, as set forth below, even assuming that such incidental collection must satisfy the Fourth Amendment's "general reasonableness" balancing test, the acquisitions at issue here were lawful under that test.

In circumstances where a warrant and probable cause are not required, searches and seizures are generally subject to the Fourth Amendment's "traditional standards of reasonableness." *King*, 133 S. Ct. at 1970; *see id.* ("To say that no warrant is required is merely to acknowledge that rather than employing a *per se* rule of unreasonableness, we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable.") (internal quotation marks and citation omitted). In assessing the constitutional reasonableness of a government search, the court must weigh "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Id.* (internal quotation marks and citation omitted); *Knights*, 534 U.S. at 117-19 (describing balancing as "general Fourth Amendment approach"); *T.L.O.*, 469 U.S. at 337 (stating that "[t]he determination of the standard of reasonableness" requires balancing). The court determines what is reasonable, and what safeguards may be necessary in a particular context, by balancing the interests at stake in light of "the totality of the circumstances." *Samson*, 547 U.S. at 848; *see also Von Raab*, 489 U.S. at 665, 668 (recognizing that "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance" and that "the traditional probable-cause standard may be unhelpful" when the government "seeks to *prevent*" dangers to public safety); *In re Directives*, 551 F.3d at 1012 (reviewing collection under the PAA under the general reasonableness test).

Under the general reasonableness balancing test, searches without a warrant or individualized finding of probable cause are particularly likely to be found reasonable when the governmental need is especially great or especially likely to be frustrated by a warrant requirement, when the search involves modest intrusions on the individual's privacy, and when alternative safeguards restrain the government within reasonable limits. *See, e.g.*, *Illinois v. McArthur*, 531 U.S. 326, 330-31 (2001) ("When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."); *King*, 133 S. Ct. at 1969 (warrantless search may be reasonable where "the public interest is such that neither a warrant nor probable cause is required" or where "an individual is already on notice . . . that some reasonable [government] intrusion on his privacy is to be expected") (citation omitted).

The Supreme Court recently engaged in this kind of balancing in *King*, which involved warrantless searches of arrestees to obtain DNA samples. *Id.* at 1968-69. The Court examined the totality of the circumstances, weighed the various interests at stake, and concluded, in light of the government's "substantial interest" in the "identification of arrestees," the diminished expectations of privacy of an individual taken into police custody, and statutory protections that limited the purposes for which the DNA evidence could be collected and stored, that the balance favored the government. *Id.* at 1977-80; *see also Samson*, 547 U.S. at 848-57 (applying reasonableness balance in upholding warrantless, suspicionless search of the person of a parolee).

The Second Circuit likewise applied the Fourth Amendment's general reasonableness test in upholding electronic surveillance abroad of a U.S. person associated with al Qaeda. *In re Terrorist Bombings*, 552 F.3d at 175-76. The court recognized that "complex, wide-ranging, and decentralized [terrorist] organizations . . . warrant sustained and intense monitoring in order to

understand their features and identify their members." *Id.* at 175. The court further observed that broad surveillance of covert terrorist organizations was necessary because such organizations "often communicate in code, or at least through ambiguous language" and that "it is not always readily apparent what information is relevant." *Id.* at 175-76. The court accordingly found, under the totality of the circumstances, that the electronic surveillance in that case was reasonable under the Fourth Amendment because, although the intrusion on the targeted U.S. person's privacy was "great," the government's national security interest in conducting the surveillance was "even greater." *Id.* at 176.

Finally, in *In re Directives*, the FISA Court of Review applied the general reasonableness test in considering the constitutional reasonableness of the PAA, the FAA's predecessor statute, in the context of an as-applied challenge brought by a private party that had been directed by the government to assist in effectuating surveillance under the statute. 551 F.3d at 1012-15.[42] In balancing the respective interests, the FISA Court of Review recognized that the government's interest in national security was of such a "high[] order of magnitude" that it would justify significant intrusions on individual privacy. *Id.* at 1012. The FISA Court of Review noted further that the PAA, the certifications, and the directives contained a "matrix of safeguards," *id.* at 1013, including "effective minimization procedures" that were "almost identical to those used under FISA to ensure the curtailment of both mistaken and incidental acquisitions," *id.* at 1015, as well as

[42] The PAA was not identical to, and in certain respects was broader than, Section 702. Notably, the PAA authorized surveillance concerning "persons reasonably believed to be outside the United States" without distinguishing between U.S.- and non-U.S. persons, *In re Directives*, 551 F.3d at 1007, while Section 702 authorizes only surveillance targeting non-U.S. persons outside the United States. In addition, the petitioner in *In re Directives* limited its claims to alleged injuries to U.S. persons. Accordingly, the analysis in *In re Directives* addresses certain issues specific to foreign intelligence surveillance targeted at U.S. persons abroad, including a requirement that surveillance targeting U.S. persons be based on a finding by the Attorney General of probable cause to believe that the U.S. person was a foreign power or agent of a foreign power, that are not applicable here.

"targeting procedures" that included "provisions designed to prevent errors" and provided for Executive Branch and congressional oversight of "compliance with the targeting procedures," *id.* The FISA Court of Review concluded, based on the panoply of safeguards in the statutory provisions and implementing procedures, that "the surveillances at issue satisfy the Fourth Amendment's reasonableness requirement." *Id.* at 1016.[43]

The FAA provisions, certification(s), and procedures at issue in this case, with respect to collection targeting non-U.S. persons overseas, are as protective as, and in some respects significantly more robust than, the comparable PAA procedures that the FISA Court of Review considered in holding that the directives issued under the PAA were constitutional.[44] In addition, the FAA goes beyond the PAA by requiring a prior finding by the FISC that the targeting and minimization procedures are reasonable under the Fourth Amendment. 50 U.S.C. § 1881a (i). The FAA, unlike the PAA, also expressly prohibits "reverse targeting" of U.S. persons or the targeting of persons "known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a (b)(1) and (2). The FAA thus stands on an even firmer constitutional foundation than the PAA, and the FISA Court of Review's analysis upholding the latter applies also to the former. The defendant's motion does not distinguish, or even cite, the FISA Court of Review's opinion in *In re Directives*.[45]

The FISC has repeatedly reviewed the targeting and minimization procedures governing the government's acquisition of foreign intelligence information under Section 702 and held that acquisitions pursuant to those procedures satisfy the Fourth Amendment reasonableness standard. *See [Caption Redacted]*, 2011 WL 10945618, at *6 ("The Court found in those prior

---

[43] *In re Directives* was not litigated *ex parte*. The FISA Court of Review considered briefing and oral argument from both the government and the communications provider that challenged the directives. 551 F.3d at 1008.

[44] [CLASSIFIED INFORMATION REDACTED]

[45] [CLASSIFIED INFORMATION REDACTED]

dockets that the targeting and minimization procedures were consistent with the requirements of [Section 702] and with the Fourth Amendment."). The only other court to have considered the question has likewise found that, in light of the "statutory protections" governing Section 702 collection, "the government's compelling interest in protecting national security outweighs the intrusion of § 702 surveillance on an individual's privacy" and therefore the Section 702 collection at issue in that case was "reasonable under the Fourth Amendment." *Mohamud*, 2014 WL 2866749, at *27. There is no reason for a different outcome here.

a. Acquisitions Under Section 702 Advance the Government's Compelling Interest in Obtaining Foreign Intelligence Information To Protect National Security

The government's national security interest in conducting acquisitions pursuant to Section 702 "is of the highest order of magnitude." *In re Directives*, 551 F.3d at 1012; *see also [Caption Redacted]*, 2011 WL 10945618, at *25; *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.") (citation omitted). The terrorist threat the United States is facing today "may well involve the most serious threat our country faces." *In re Sealed Case*, 310 F.3d at 746; *see also Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2724 (2010) ("[T]he Government's interest in combating terrorism is an urgent objective of the highest order."); *Duka*, 671 F.3d at 340 ("The government's interests in security and intelligence are entitled to particular deference."). Courts have recognized that the government's compelling interest in collecting foreign intelligence information to protect the Nation against terrorist groups and other foreign threats may outweigh individual privacy interests. *See, e.g., In re Terrorist Bombings*, 552 F.3d at 175 (recognizing the government's "compelling" interest in conducting "sustained and intense" surveillance of foreign

terrorist organizations); *Cassidy*, 471 F.3d at 82 (upholding warrantless searches of ferry passengers in light of government interest in "[p]reventing or deterring large-scale terrorist attacks").

The collection authorized by Section 702 is crucial to the government's efforts against terrorism and other threats both to the United States and its interests abroad. *See* National Security Agency, *The National Security Agency: Missions, Authorities, Oversight and Partnerships* 4 (August 9, 2013), available at www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf ("[C]ollection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."). As the Senate Select Committee on Intelligence found in recommending re-authorization of the FAA in 2012, "the authorities provided under the FAA have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets." S. Rep. No. 112-174, at 2 (2012); *see also id.* at 17 (noting that Section 702, in addition to "provid[ing] information about the plans and identities of terrorists" also enables the government to collect "information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States"). The Committee noted further that "failure to reauthorize Section 702" would "result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities." *Id.*; *see also* H.R. Rep. 112-645 (II), at 3 (Aug. 2, 2012) ("The importance of the collection of foreign intelligence under the FAA . . . cannot be underscored enough. . . . The information collected under this authority is often unique, unavailable from any other source, and regularly provides critically important insights and

operationally actionable intelligence on terrorists and foreign intelligence targets around the world.").[46]

The PCLOB found that Section 702 has "proven valuable in a number of ways to the government's efforts to combat terrorism." PCLOB Report at 107. The PCLOB noted that "over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection," and that Section 702 collection is a uniquely valuable tool in enabling the government to discover and monitor terrorist networks despite the terrorists' efforts to conceal their activities and communications. *Id.* at 104-08. The PCLOB reviewed numerous specific instances in which Section 702 collection contributed to a counterterrorism investigation and found that information obtained through Section 702 has played a key role in "the discovery of previously unknown terrorist plots" and has "directly enabled the thwarting of specific terrorist attacks, aimed at the United States and at other countries." *Id.* at 108-09. Finally, the PCLOB noted that Section 702 has also proven "highly valuable" in serving foreign intelligence purposes other than preventing terrorism, including countering the efforts of proliferators of weapons of mass destruction. *Id.* at 110. Thus, as the Executive Branch, Congress, the FISC, and the PCLOB have

---

[46] *Amici* contend (Br. 24-25) that Section 702 collection is unreasonable because there are "reasonable alternatives," including requiring a warrant before "accessing Americans' communications" collected under Section 702, that would serve the government's foreign intelligence needs while providing greater protections to privacy interests. However, the Supreme Court has "repeatedly refus[ed] to declare that only the 'least intrusive' search practicable can be reasonable." *City of Ontario v. Quon*, 560 U.S. 746, 763 (2010). Moreover, as the PCLOB found, the "greater degree of flexibility" afforded by Section 702 is important to the government's foreign intelligence interests because it "allow[s] the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court" for specific targeting (or querying) actions. PCLOB Report at 106. The warrant requirement suggested by *amici* would hinder that flexibility and make more difficult the "sustained and intense surveillance" of foreign terrorist groups that is of vital interest to the safety of the Nation. *See In re Terrorist Bombings*, 552 F.3d at 175.

all recognized, the government has an extraordinarily compelling interest in conducting the collection authorized by Section 702.

b. Persons in the United States Have Limited Expectations of Privacy in Electronic Communications With Non-U.S. Persons Outside the United States

The other side of the Fourth Amendment reasonableness balance is the degree to which the search "intrudes upon an individual's privacy." *Knights*, 534 U.S. at 118-19 (citation omitted). Where the search takes place in circumstances in which the individual's expectations of privacy are limited, the diminished character of the privacy interest must be taken into account in the court's assessment of reasonableness.

Because surveillance under Section 702 must target non-U.S. persons reasonably believed to be located outside the United States (who generally lack Fourth Amendment rights), the only constitutional interests at stake are those of persons protected by the Fourth Amendment who were either mistakenly targeted under Section 702, or whose communications were incidentally collected in the course of the government's targeting of another person reasonably believed to be a non-U.S. person outside the United States. In the context of incidental collection, the privacy interests of U.S. persons in communications are significantly diminished when those communications have been transmitted to or obtained from non-U.S. persons located abroad.

The Supreme Court has long held that when one person voluntarily discloses information to another, the first person loses any cognizable interest under the Fourth Amendment in what the second person does with the information. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *Couch v. United States*, 409 U.S. 322, 335 (1973); *White*, 401 U.S. at 752 (plurality opinion); *Hoffa v. United States*, 385 U.S. 293, 302-03 (1966). For Fourth Amendment purposes, the same principle applies whether the recipient intentionally makes the information public or stores

it in a place subject to a government search. Thus, once a non-U.S. person located outside the United States receives information, the sender generally loses any cognizable Fourth Amendment rights with respect to that information. That is true even if the sender is a person protected by the Fourth Amendment, because he assumes the risk that the foreign recipient will give the information to others, leave the information freely accessible to others, or that the U.S. government (or a foreign government) will obtain the information.[47]

This rule applies to physical mail, even within the United States. Although the Fourth Amendment protects sealed letters in transit, "once a letter is sent to someone, 'the sender's expectation of privacy ordinarily terminates upon delivery.'" *United States v. Gordon*, 168 F.3d 1222, 1228 (10th Cir. 1999) (quoting *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995)). The same rule applies to email users, who lack a legitimate expectation of privacy in an email that has already reached its recipient. *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (recognizing that, while "[i]ndividuals generally possess a reasonable expectation of privacy in their home computers," there is no such "expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient"); *see also Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001).[48]

---

[47] The "recipient" in this context refers to the ultimate recipient, not (for example) an internet service provider. *See United States v. Warshak*, 631 F.3d 266, 282-88 (6th Cir. 2010). Thus, while *Warshak* held that a subscriber has a reasonable expectation of privacy in emails that the provider stores in the *subscriber's* account, it did not say that a person's Fourth Amendment rights are implicated when the government obtains, from the service provider, emails from *someone else*'s account.

[48] Moreover, any expectation of privacy of the defendant in his electronic communications with a non-U.S. person overseas is also diminished by the prospect that his foreign correspondent could be a target for surveillance by foreign governments or private entities, whose activities are not governed by the United States Constitution or federal law, or by the U.S. Government, pursuant to various authorities applicable to foreign intelligence surveillance conducted abroad. *Cf. Clapper*, 133 S. Ct. at 1149 (noting that the government conducts surveillance of persons abroad under "programs that are governed by Executive Order 12333" and that "[t]he Government may also obtain information

[CLASSIFIED INFORMATION REDACTED]

Finally, the principles underlying the "border search" doctrine are also relevant to this Court's weighing of the individual's privacy interests relative to the government's interests in this context. Courts have long recognized the government's paramount interest in examining persons and property entering or exiting the country. *Flores-Montano*, 541 U.S. at 152. In that context, "not only is the expectation of privacy less," but also "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government." *United States v. Montoya de Hernandez*, 473 U.S. 531, 539-40 (1985) (citation omitted). Accordingly, under the rubric of the "border search" doctrine, courts have long recognized a diminished expectation of privacy in letters or packages that transit an international border, even where the search takes place in the interior of the country. *See United States v. Ramsey*, 431 U.S. 606, 620 (1977) (holding that the border search exception applies to international letters, because "[t]he critical fact is that the envelopes cross the border . . . not that they are brought in by one mode of transportation rather than another"); *United States v. Seljan*, 547 F.3d 993, 1003 (9th Cir. 2008) ("An envelope containing personal correspondence is not uniquely protected from search at the border."); *United States v. King*, 517 F.2d 350, 354 (5th Cir. 1975) ("Appellants here could have had no reasonable expectation that their letters, mailed from abroad, would remain uninspected.").

---

from the intelligence services of foreign nations"); *Amnesty Int'l. USA v. Clapper*, 667 F.3d 163, 192 (2d Cir. 2011) (Raggi, J., dissenting) (Because "the United States is hardly the only government conducting electronic surveillance," the foreign contacts of plaintiffs challenging the FAA might "be prime targets for surveillance by other countries," especially foreign contacts "believed to be associated with terrorist organizations."); *Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring) (noting the relevance of "differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad") This reality, which courts have acknowledged, arguably put the defendant "on notice . . . that some reasonable [government] intrusion on his privacy is to be expected." *King*, 133 S. Ct. at 1969.

The same rationale applies also to international data transmissions, like the communications at issue here, because such transmissions, in the form of terrorist communications, cyber attacks, illegal financial transactions, and the like, may implicate national security or other government interests to a similar degree as physical mail in an envelope. *See Seljan*, 547 F.3d at 1001-03 (upholding suspicionless search of envelope containing personal correspondence in light of "tempered" expectation of privacy in international mail and the government's interest in "regulating the flow of persons and property across the border."). Although the government does not contend that the Section 702 collection here was per se reasonable under the border search doctrine, the point remains that the principles underlying that doctrine support the constitutional reasonableness of the collection at issue in this case.

c. The Privacy Interests of U.S. Persons Are Protected by Stringent Safeguards and Procedures

The government employs multiple safeguards that are designed to ensure that surveillance is appropriately targeted at non-U.S. persons located outside the United States for foreign intelligence purposes and to protect the privacy interests of U.S. persons who communicate with targets or whose communications are otherwise incidentally collected. These safeguards and procedures – some of which go beyond what courts have held reasonable in the context of "special needs" warrantless searches involving less compelling governmental interests – provide constitutionally sufficient protection for the privacy interests of persons protected by the Fourth Amendment.

i. Senior officials certify that the government's procedures satisfy statutory requirements

Section 702 requires the DNI and the Attorney General to certify that procedures are in place to protect the privacy of U.S. persons and non-U.S. persons located in the United States,

including targeting procedures and minimization procedures. 50 U.S.C. § 1881a(a), (g), and (i). In addition, the DNI and Attorney General must also certify, *inter alia*, that a significant purpose of the acquisition is to obtain foreign intelligence information, that the Attorney General and DNI have adopted guidelines to ensure compliance with the statutory limitations in Section 702(b), and that the targeting procedures, minimization procedures, and guidelines adopted by the government are consistent with the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(A). The requirement that these senior executive branch officials certify that the procedures comply with statutory requirements and with the Constitution represents an important "internal check" on the actions of the Executive Branch. *See In re Sealed Case*, 310 F.3d at 739.

ii. Targeting procedures ensure that the government targets only non-U.S. persons reasonably believed to be outside the United States

Section 702 provides that the targeting procedures must be "reasonably designed" to "ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *See* 50 U.S.C. § 1881a(d)(1). The FISC repeatedly has found that the targeting procedures employed by the government meet that standard. *See supra* Part V.B.; *[Caption Redacted]*, 2011 WL 10945618, at *6 ("The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of 50 U.S.C. § 1881(d)-(e) and with the Fourth Amendment.").

[CLASSIFIED INFORMATION REDACTED]

These detailed procedures refute the defendant's contention that collection under Section 702 is unreasonably broad because it authorizes the government to "target entire

geographical areas." (Def. Mot. 23). That contention is groundless because, under the targeting procedures, "selectors are always unique communications identifiers used by the targeted persons." PCLOB Report at 111-12; *see also id.* at 112 ("[T]he government is not creatively interpreting the meaning of 'selectors' to engage in bulk collection under Section 702."). Those contentions amount to an accusation that the government will intentionally not abide by the required procedures, despite extensive oversight, and that the government will intentionally engage in "reverse targeting" of U.S. persons or persons reasonably believed to be located in the United States, even though that is expressly prohibited by the statute, *see* 50 U.S.C. § 1881a(b)(2). Moreover, as the FISA Court of Review recognized, there is a "presumption of regularity" that "supports the official acts of public officers," and unless there is "clear evidence to the contrary, courts presume that they have properly discharged their official duties." *In re Directives*, 551 F.3d at 1011; *see also Mohamud*, 2014 WL 2866749, at *21 (applying the presumption of regularity to Section 702 collection and finding "no evidence" of misconduct). In this case, as set forth more fully *infra*, there is no indication of non-compliance with respect to the collection at issue that would rebut that presumption.[49]

[CLASSIFIED INFORMATION REDACTED]

iii. Minimization procedures protect the privacy of U.S. persons whose communications are acquired

Section 702 requires the government to employ minimization procedures, as defined in FISA, to limit the acquisition, retention, and dissemination of information concerning U.S. persons. *See* 50 U.S.C. § 1801(h)(1). Section 702 further requires that the FISC review those procedures and determine that acquisitions in accordance with such procedures would be consistent with the FAA and the Fourth Amendment. 50 U.S.C. § 1881a(i)(1) and (2).

[49] [CLASSIFIED INFORMATION REDACTED]

The minimization procedures governing Section 702 collection, some of which have recently been declassified, are appropriately designed to minimize the acquisition, retention, and dissemination of information to, from, or about U.S. persons, consistent with the government's foreign intelligence needs. *See Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended*, October 31, 2011), available at www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf ("NSA 2011 Minimization Procedures").[50] The procedures further require, among other things, that the identity of U.S. persons be redacted from intelligence reports prior to dissemination unless the information constitutes foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime. *Id.* § 6(b). In other words, the procedures by design aim to ensure that any intrusion on the privacy of U.S. persons is reasonably balanced against the government's intelligence and law enforcement needs.

For the same reasons that courts have found the use of minimization procedures to be an important factor in holding traditional FISA surveillance to be reasonable under the Fourth Amendment, *In re Sealed Case*, 310 F.3d at 740-42, the use of substantially similar minimization procedures supports the reasonableness of surveillance under Section 702. *In re Directives*, 551 F.3d at 1015 (finding it "significant," in upholding the PAA, that "effective minimization procedures are in place" to "serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons");

[50] [CLASSIFIED INFORMATION REDACTED]

Mohamud, 2014 WL 2866749, at *23 (holding that "the minimization procedures contribute to the reasonableness of § 702 under the Fourth Amendment").[51]

Amici contend (Br. at 22-23; *see also* Def. Mot. 6) that the minimization protections are inadequate because the FISC approves standard minimization procedures governing all collection under the particular certification, rather than fashioning "instance specific" minimization procedures for each target. However, Congress has recognized that the application of uniform minimization procedures to collection directed against multiple targets actually *enhances* the protection of U.S. person information. H.R. Rep. No. 95-1283, Pt. 1, at 75 (1978)("It is the intention of the committee that minimization procedures be as uniform as possible for similar surveillances. . . . The application of uniform procedures to identical surveillances will result in a more consistent implementation of the procedures, will result in an improved capability to assure compliance with the procedures, and ultimately means a higher level of protections for the rights of U.S. persons."); *see United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 303 n.4 (D. Conn. 2008), *aff'd* 630 F.3d 102 (2d Cir. 2010) (noting that "the Attorney General has adopted standard minimization procedures that apply to every [Title I] FISA application"); *In re All Matters Submitted to Foreign Intelligence Surveillance Ct.*, 218 F. Supp. 2d 611, 615 (FISC 2002) (referring to "Standard Minimization Procedures for a U.S. Person Agent of a Foreign Power that are filed with the Court, which we continue to approve"). The sufficiency of the minimization procedures therefore does not depend on the identity of the particular target, but rather on whether the procedures are reasonably designed "in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination" of information about United States persons consistent with

[51] [CLASSIFIED INFORMATION REDACTED]

the government's need to obtain, produce, and disseminate foreign intelligence information. 50 U.S.C. §§ 1801(h)(1), 1821(4)(A); *see* 50 U.S.C. § 1881a(e)(1).

Contrary to *amici*'s claim (Br. at 22), the minimization procedures employed here provide materially equivalent protection to the procedures employed for Title I and III FISA collection, and courts have found that these procedures sufficiently protect the privacy interests of U.S. persons whose communications are incidentally acquired. *In re Sealed Case*, 310 F.3d at 740-41; *see In re Directives*, 551 F.3d at 1015 (recognizing as "significant" to the Court's finding that acquisitions under the PAA were reasonable, that "effective minimization procedures are in place" that were "almost identical" to those used in traditional FISA surveillance); *Mohamud*, 2014 WL 2866749, at *24 (rejecting defendant's contention that Section 702's minimization procedures "provide no meaningful protection" and holding that "the minimization procedures contribute to the reasonableness of § 702 under the Fourth Amendment"). In addition, those procedures have repeatedly been found sufficient in the context of traditional FISA electronic surveillance and physical searches, which target persons in the United States and therefore are more likely to capture communications of non-targeted U.S. persons than the foreign communications targeted under Section 702. *See [Caption Redacted]*, 2011 WL 10945618, at *7.

[CLASSIFIED INFORMATION REDACTED]

Amici contend (Br. at 21-22) that the minimization procedures are inadequate because they permit the government to query information already collected pursuant to Section 702 using terms associated with U.S. persons.[52] The defendant's contention is incorrect on the merits.

Courts have held in various contexts that where the government's querying of information that has lawfully been obtained does not implicate any reasonable expectation of privacy

[52] [CLASSIFIED INFORMATION REDACTED]

beyond that implicated in the initial collection, merely running queries in a database does not infringe on any significant privacy interest or trigger any fresh constitutional analysis. *See Boroian v. Mueller*, 616 F.3d 60, 67-68 (1st Cir. 2010) ("[T]he government's retention and matching of [an individual's] profile against other profiles in [a DNA database] does not violate an expectation of privacy that society is prepared to recognize as reasonable, and thus does not constitute a separate search under the Fourth Amendment"); *see also Johnson v. Quander*, 440 F.3d 489, 498-99 (D.C. Cir. 2006) (holding that "accessing the records stored in the [DNA] database is not a 'search' for Fourth Amendment purposes" based in part on cases holding that, where a photograph is "taken in conformance with the Fourth Amendment, the government's storage and use of it does not give rise to an independent Fourth Amendment claim."). Notably, the Sixth Circuit has applied this principle in the foreign intelligence context. *Jabara v. Webster*, 691 F.2d 272, 277-79 (6th Cir. 1982) (holding, where plaintiff did not challenge the lawfulness of warrantless NSA interception of his foreign communications but challenged only the subsequent dissemination of the communications to the FBI, that such dissemination "after the messages had lawfully come into the possession of the NSA" did not implicate any reasonable expectation of privacy).[53]

The same reasoning applies here. Where the government has lawfully collected foreign intelligence information pursuant to statutory requirements and FISC-approved procedures that meet Fourth Amendment standards, the government's subsequent querying of that information

[53] A rule that every query, dissemination, or use of Section 702-obtained information amounts to a separate search under the Fourth Amendment would not only be contrary to these cases but also would be impracticable, because, as the Sixth Circuit explained in *Jabara*, such a rule would require "a succession of warrants as information, lawfully acquired, is passed from one agency to another." 691 F.2d at 279; *see also id.* at 277 ("Evidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken.") (citation omitted). Accordingly, "[A]n expectation that information lawfully in the possession of a government agency will not be disseminated, without a warrant, to another government agency is [not] an expectation of privacy that society is prepared to recognize as reasonable." *Id.* at 279.

does not amount to a significant further intrusion on privacy that implicates the Fourth Amendment. *See King*, 133 S. Ct. at 1980 (holding, "in light of the scientific and statutory safeguards" governing Maryland's warrantless collection of DNA from persons arrested for serious offenses, that "once respondent's DNA was lawfully collected," the subsequent analysis of the DNA "did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment"). Accordingly, the government's querying of information lawfully obtained pursuant to Section 702 does not amount to a separate search under the Fourth Amendment and does not require separate or additional judicial process.

Finally, the fact that minimization procedures may permit the government to query information lawfully collected pursuant to Section 702 using identifiers associated with U.S. persons does not render those procedures constitutionally unreasonable. *See Mohamud*, 2014 WL 2866749, at *24-*26 (holding that, although it is a "close question," the "subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment"). First, as noted above, the querying of information that the government lawfully has obtained is not a significant additional intrusion on a person's privacy, beyond the level of intrusion that has already resulted from the government's collection and review of the information pursuant to court-approved targeting and minimization procedures. Consistent with those procedures, the government is of course permitted to review the information it lawfully collects under Section 702 – which includes information concerning U.S. persons – to assess whether the information should be retained or disseminated. Accordingly, U.S.-person information is, by necessity, already subject to review (and use) under the FISC-approved minimization procedures. It would be perverse to authorize the unrestricted review of lawfully collected information but then to restrict the targeted review of the same information in response to

tailored queries. *See* PCLOB Report at 131 ("[R]ules and oversight mechanisms are in place to prevent U.S. person queries from being abused for reasons other than searching for foreign intelligence information or, in the FBI's case, for evidence of a crime."). Querying lawfully collected information using U.S.-person identifiers does not involve a significant additional intrusion on a person's privacy, beyond the level of intrusion already occasioned by the government as it reviews and uses information it lawfully collects under Section 702 pursuant to its need to analyze whether the information should be retained or disseminated.

On the other side of the balance, the government has a powerful interest in conducting such queries for appropriate purposes including, for example, discovering potential links between foreign terrorist groups and persons within the United States in order to detect and disrupt terrorist attacks.[54] Similarly, the government's interest in preventing crime is "paramount," and a criminal investigation is always a "compelling" state interest. *Branzburg v. Hayes,* 408 U.S. 665, 700 (1972); *see also In re Directives*, 551 F.3d at 1011 ("A surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose" because, for example, the "apprehension of terrorism suspects . . . is inextricably intertwined with the national security concerns that are at the core of foreign intelligence collection."). Likewise, the FISC repeatedly has approved minimization procedures that permit queries using U.S. person identifiers. *See [Caption Redacted]*, 2011 WL 10945618, at *7. In approving such queries in the context of Section 702 collection, the FISC noted that the minimization procedures applicable to certain other FISA-acquired information, which the FISC had previously approved, similarly permit queries using U.S. person identifiers, even though that information was likely to include a higher concentration of U.S.

[54] Such queries also help the government counteract operational security measures such as hiding operational communications in large amounts of non-operational communications in the hope of delaying the government's detection of those communications.

person information than Section 702 collection. *Id.* The FISC concluded, "[i]t follows that the substantially-similar querying provision found [in] the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons." *Id.*[55]

[CLASSIFIED INFORMATION REDACTED]

iv. A significant purpose of the acquisition must be to obtain foreign intelligence information

Section 702 only authorizes collection when a "significant purpose" of the collection is to "obtain foreign intelligence information." 50 U.S.C. § 1881a(g)(2)(A)(v). That requirement precludes the government from using directives issued under Section 702 "as a device to investigate wholly unrelated ordinary crimes." *In re Sealed Case*, 310 F.3d at 736. The targeting procedures ensure that any surveillance satisfies this purpose requirement by requiring, through consideration of a range of factors, an assessment that the individual or facility targeted for collection is likely to communicate foreign intelligence information.[56] *See* PCLOB Report at 45. These requirements appropriately limit the scope of the acquisition and support the reasonableness of collections under Section 702. *See In re Directives*, 551 F.3d at 1013 (recognizing "a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information" as among the procedural safeguards supporting the PAA's reasonableness under the Fourth Amendment); *Mohamud*, 2014 WL 2866749, at *27 (same as to Section 702).[57]

[55] [CLASSIFIED INFORMATION REDACTED]

[56] [CLASSIFIED INFORMATION REDACTED]

[57] [CLASSIFIED INFORMATION REDACTED]

v. Executive Branch, Congressional, and Judicial Oversight

Section 702 requires the Attorney General and DNI to periodically assess the government's compliance with both the targeting and minimization procedures and with relevant compliance guidelines. *See* 50 U.S.C. § 1881a(*l*). They must submit those assessments both to the FISC and to congressional oversight committees. *Id.* The Attorney General must also keep the relevant oversight committees "fully inform[ed]" concerning the implementation of Section 702. 50 U.S.C. § 1881f(a) and (b)(1); *see also Clapper*, 133 S. Ct. at 1144 ("Surveillance under § 1881a is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment.").

In 2012, the Senate Select Committee on Intelligence, following four years of such oversight, found that

> [T]he assessments, reports, and other information obtained by the Committee demonstrate that the government implements the FAA surveillance authorities in a responsible manner with relatively few incidents of non-compliance. Where such incidents have arisen, they have been the inadvertent result of human error or technical defect and have been promptly reported and remedied. Through four years of oversight, the Committee has not identified a single case in which a government official engaged in a willful effort to circumvent or violate the law. Moreover, having reviewed opinions by the FISA Court, the Committee has also seen the seriousness with which the Court takes its responsibility to carefully consider Executive Branch applications for the exercise of FAA surveillance authorities.

S. Rep. No. 112-174, at 7 (2012); *see also* H.R. Rep. No. 112-645 (II), at. 4 (2012) ("The oversight this committee has conducted since the FAA was enacted in 2008 has shown no evidence that the Intelligence Community has engaged in any intentional or willful failure to comply with statutory requirements or Executive Branch policies and procedures."); PCLOB Report at 11 ("The Board has seen no trace" of any attempted "exploitation of information acquired under [Section 702] for illegitimate purposes" nor "any attempt to intentionally circumvent legal limits."). Under the FAA, as in traditional FISA, the "in-depth oversight of FISA surveillance by all three branches of

government" helps to "ensure[]" the "privacy rights of individuals" and to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982). This extensive oversight, and the resulting findings of Congress, the FISC, and the PCLOB, refute the defendant's contention (Def. Mot. 6) that Section 702 "fails to provide any accountability" over the government's conduct of Section 702 surveillance.

vi. Prior Judicial Review

Finally, Section 702 requires the FISC to enter an order approving the certification and the use of the targeting and minimization procedures if the court finds that the certification contains all the required elements, and that the targeting and minimization procedures are consistent with the requirements of 50 U.S.C. §§ 1881a(d) and (e) and with the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A). The requirement of prior FISC approval, and in particular the requirement of a judicial finding that the government's targeting and minimization procedures are consistent with the Fourth Amendment, support the conclusion that Section 702 collection conducted pursuant to such procedures is constitutional. *See Clapper*, 133 S. Ct. at 1150 (noting the importance of the requirement that the FISC "assess whether the Government's targeting and minimization procedures comport with the Fourth Amendment"); *see also Clapper*, 667 F.3d at 190 (Raggi, J., dissenting) ("There is no reason to think that the Article III judges who serve on the FISA court will be timid in exercising this review authority"). Indeed, the FISC's declassified opinions make clear that the FISC rigorously reviews the constitutional reasonableness of the applicable procedures and subjects those procedures to exacting scrutiny. *See, e.g., [Caption Redacted]*, 2011 WL 10945618; PCLOB Report 26-31 (describing how the FISC's review is informed by the government's compliance reports, witness testimony at hearings, and other submissions, which enable the court to review the

targeting and minimization procedures "as actually applied by the Intelligence Community to particular, real-life factual scenarios"). The FISC's history of conducting rigorous and detailed review refutes defendant's attempt (Def. Mot. 29, 43-44) to disparage the FISC's role as "merely . . . ratifying Executive Branch decisions."

The defendant also contends (Def. Mot. 29-30) that the FISC's assessment of Section 702 certifications and corresponding targeting and minimization procedures results in "impermissible advisory opinion[s]." He is incorrect.

"Article III courts perform a variety of functions not necessarily or directly connected to adversarial proceedings in a trial or appellate court." *Mistretta v. United States*, 488 U.S. 361, 389 n.16 (1989); *see also Morrison v. Olson*, 487 U.S. 654, 679 n.16 (1988). In particular, the courts have long participated in the oversight of government searches and surveillance by reviewing warrant and wiretap applications, notwithstanding that these proceedings are wholly *ex parte* and do not occur at the behest of an aggrieved party as ordinarily required for a "case or controversy" under Article III. *Mistretta*, 488 U.S. at 389 n.16; *see also, e.g.*, *In re Sealed Case*, 310 F.3d at 732 n.19 ("In light of [*Morrison* and *Mistretta*], we do not think there is much left to an argument . . . that the statutory responsibilities of the FISA court are inconsistent with Article III case and controversy responsibilities of federal judges because of the secret, non-adversary process.").

Congress's decision to vest the FISC with jurisdiction to review the reasonableness of procedures for searches or surveillance under the FAA is perfectly consistent with the traditional function of Article III courts in protecting the privacy rights of persons whose interests are potentially implicated by proposed searches, seizures, or compulsory processes. *Mohamud*, 2014 WL 2866749, at *10 (noting that the FISC's "[r]eview of § 702 surveillance applications is as

central to the mission of the judiciary as the review of search warrants and wiretap applications"); *see also In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 144 (E.D. Va. 2011) ("Grand Juries, search warrants, wiretap orders, and many other *ex parte* applications and orders rely on judicial review to protect the rights of potential subjects of investigation. All of these tools have been routinely and consistently approved by the courts.")

Moreover, the decision the FISC is called upon to render under Section 702 is not merely "advisory," any more than a decision on a traditional search warrant or wiretap application is "advisory." If the FISC disapproves the government's proposed targeting or minimization procedures under Section 702, that decision has legal effect, because it bars the government from conducting collections under the statute if it does not remedy the deficiency within thirty days. A FISC order approving the proposed certification and procedures also has an effect on third parties, because it authorizes the government to issue directives (compulsory process analogous to a subpoena) to electronic communications service providers. The fact that the providers have a right to challenge a directive in court further establishes that a FISC order approving a Section 702 certification is not an advisory opinion but a legally enforceable order potentially subject to legal challenge. *See Clapper*, 133 S. Ct. at 1154 ("[A]ny electronic communications service provider that the Government directs to assist in § 1881a surveillance may challenge the lawfulness of that directive before the FISC."). *Mohamud*, 2014 WL 2866749, at *11 (rejecting defendant's argument that "FISC judges only provide advisory opinions"). In sum, "FISC review of § 702 surveillance submissions provides prior review by a neutral and detached magistrate," which serves to "strengthen[]" rather than "undermine[]" any Fourth Amendment interests implicated by the collection. *Mohamud*, 2014 WL 2866749, at *11.

d. Collection Under Section 702 Has Sufficient Particularity

The defendant's overarching argument is, in essence, that collection pursuant to Section 702 fails the Fourth Amendment's general reasonableness test because it does not require a particularized court order or finding of probable cause as in traditional FISA collection or domestic law enforcement wiretaps under Title III. (Def. Mot. 6-8). In doing so, the defendant characterizes Section 702-authorized collection as "dragnet" surveillance that collects communications in bulk. (*See, e.g.*, *id.* at 14, 25). However, collection under Section 702 is *not* bulk collection. *See* PCLOB Report at 111 ("[T]he Section 702 program is not based on the indiscriminate collection of information in bulk" because "the program consists entirely of targeting specific persons about whom an individualized determination has been made."); *see also id.* at 103 ("The [Section 702] program does not operate by collecting communications in bulk."). Section 702 collection is targeted and particularized because FISC-approved procedures require the government to determine (1) that the particular "user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States," *[Caption Redacted]*, 2011 WL 10945618, at *7; and (2) the collection is designed to obtain foreign intelligence information within the scope of the certification approved by the court.[58] Thus, as the PCLOB noted, the government

[58] Indeed, a review of "transparency reports" recently published by various U.S. Internet Service Providers demonstrates that collection of communications' content pursuant to FISA orders and FAA directives is far from bulk "dragnet" surveillance. For example, Microsoft reported receiving "fewer than 1,000 FISA orders" (which Microsoft defines to include both traditional FISA orders and FAA directives that were received or active during the reporting period) that related to between 16,000 and 16,999 user accounts during the six-month period between July and December 2012. *See* Brad Smith, General Counsel and Executive Vice President, Legal and Corporate Affairs, Microsoft, *Providing additional transparency on U.S. government requests for customer data* (Feb. 3, 2014), available at http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/02/03/providing-additional-transparency-on-US-government-requests-for-customer-data.aspx. A particular user may have multiple accounts, so this "does not necessarily mean that more than [16,000] people were covered by these data requests." *Id.* Rather, "this number will likely overstate the number of individuals subject to government orders." *Id.* The number of user accounts impacted by the same

must determine that a *specific* non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information and that the person uses a *specific* communications "selector," such as an email address or telephone number, and the government acquires only communications involving that particular selector. PCLOB Report at 20-23, 32-33, 111-12.

[CLASSIFIED INFORMATION REDACTED]

Moreover, the defendant's argument (Def. Mot. 5-9, 15-16) conflates the test for constitutional reasonableness with the *different* requirements for a warrant under the Fourth Amendment. In *In re Directives*, the FISA Court of Review rejected the petitioner's "invitation to reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable." 551 F.3d at 1013. Although particularity may be considered as one factor among many in assessing the reasonableness of a particular search, the Fourth Amendment "imposes no irreducible requirement" of individualized suspicion where the search is otherwise reasonable, as it is here. *See King*, 133 S. Ct. at 1969. Moreover, as the FISA Court of Review found in the context of the PAA, the "matrix of safeguards," including robust targeting and minimization procedures, provide constitutionally sufficient protections for the same interests that would be served by requirements of particularity or prior judicial review of individual targets. *In re Directives*, 551 F.3d at 1013.

In sum, in enacting Section 702, Congress and the Executive Branch developed a framework of procedures to facilitate collection of foreign intelligence vital to the nation's security

---

number of orders during other six-month reporting periods was even less, namely up to 15,999 between January and June 2013 and up to 11,999 between July and December 2011 and January to June 2012. *Id.* When balanced against the "hundreds of millions" of Microsoft customers, "only a fraction of a percent of [Microsoft] users are affected by these orders. In short, this means that we have not received the type of bulk data requests that are commonly discussed publicly regarding telephone records." *Id.*

while protecting any constitutionally protected privacy interests implicated by the collection. That framework - which protects civil liberties before, during and after collection - is entitled to the utmost constitutional respect by this Court. *See Youngstown*, 343 U.S. at 635-37 (Jackson, J., concurring); *In re Directives*, 551 F.3d at 1016 ("[W]here the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts."). The safeguards built into the statute and the certifications and procedures by which it was implemented here ensured that the collection targeted only foreign person(s) outside the United States and was conducted in a way that only incidentally implicated the privacy of U.S. persons. Evaluating the totality of the circumstances and weighing the compelling governmental interests at stake in combination with the extensive safeguards employed by the government to protect the privacy interests of U.S. persons – including (1) certifications by Executive Branch officials concerning the permissible foreign intelligence purposes of the collection; (2) targeting procedures designed to ensure that only non-U.S. persons abroad are targeted; (3) minimization procedures to protect the privacy of U.S. persons whose communications are incidentally acquired; (4) the requirement of a significant purpose to obtain foreign intelligence information; (5) extensive oversight within the Executive Branch, as well as by Congress and the FISC; and (6) a prior judicial finding that the targeting and minimization procedures are consistent with the Fourth Amendment – this Court should hold that the government's acquisition pursuant to Section 702 of the foreign intelligence information challenged by the defendant meets the Fourth Amendment's central requirement of reasonableness.

B. THE GOOD FAITH EXCEPTION APPLIES

The good-faith exception to the exclusionary rule set forth in *United States v. Leon*, 468 U.S. 897, 913 (1984), provides an independent basis for denying the defendant's suppression motion. *See, e.g., United States v. Ning Wen*, 477 F.3d 896, 897-98 (7th Cir. 2007) (applying good-faith exception to a claim that FISA surveillance violated the Fourth Amendment). The good-faith rule applies when law enforcement agents act in "objectively reasonable reliance on a statute" authorizing warrantless searches that is later deemed unconstitutional, *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987), when law enforcement officers reasonably rely on the probable-cause determination of a neutral magistrate, *see Leon*, 468 U.S. at 920, and when law enforcement officers reasonably rely on then-binding appellate precedent that is subsequently overturned, *see Davis v. United States*, 131 S. Ct. 2419, 2434 (2011).

The good-faith exception applies here because the collection at issue was authorized by a duly enacted statute, an order issued by a neutral magistrate, and court of appeals precedent. *Mohamud*, 2014 WL 2866749, at *30 (holding that the good-faith exception applies to Section 702 surveillance conducted in reliance on the statute and a FISC-approved certification). First, government agents conducted the collection at issue here pursuant to Section 702, as well as under procedures adopted by the Attorney General pursuant to the statute. *See Krull*, 480 U.S. at 349; *Duka*, 671 F.3d at 346 (reasoning that the good-faith rule applies because the search "was conducted in objectively reasonable reliance on a duly authorized statute [FISA]"); *see also United States v. Marzook*, 435 F. Supp. 2d 778, 790-91 (N.D. Ill. 2006) (holding that "the FBI's reliance on the Attorney General's approval under Executive Order No. 12333 — an order that no court has found unconstitutional — was [ ] objectively reasonable because that order pertains to foreign intelligence gathering"). Second, the agents also reasonably relied on orders issued by neutral magistrates — the

judges of the FISC — who repeatedly have held that the applicable targeting and minimization procedures are reasonable under the Fourth Amendment. *See Leon*, 468 U.S. at 920; *see also Duka*, 671 F.3d at 347 n.12 ("[O]bjective . . . reliance on the statute in this case is further bolstered by the fact that the particular provision at issue has been reviewed and declared constitutional by several courts."); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 140 n.12 (D. Mass. 2007) (applying the good-faith exception because "there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on the FISA orders"). Finally, the agents reasonably relied on appellate precedent from the FISA Court of Review that upheld similar directives issued under the PAA. *See Davis*, 131 S. Ct. at 2433-34; *In re Directives*, 551 F.3d at 1016.

The defendant cannot show that Section 702 is so "clearly unconstitutional," *Krull*, 480 U.S. at 349, that "a reasonable officer should have known that the statute was unconstitutional," *id.* at 355. Nor can he show that the collection was the result of "systemic error or reckless disregard of constitutional requirements." *Herring v. United States*, 555 U.S. 135, 147 (2009). Accordingly, even if the collection were deemed unconstitutional, the evidence derived from that collection would not be subject to exclusion.[59]

[59] In the related context of Title III of the Wiretap Act, the weight of the precedent establishes that Title III's statutory suppression remedy for criminal wiretap orders incorporates the good-faith exception. *See United States v. Moore*, 41 F.3d 370, 374, 376 (8th Cir. 1994) (applying good-faith exception to Title III violation); *United States v. Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988) (same); *United States v. Brewer*, 204 Fed. Appx. 205 (4th Cir. 2006) (same); *United States v. Solomonyan*, 451 F. Supp. 2d 626, 637-38 (S.D.N.Y. 2006) (collecting cases). Although two courts of appeals have held otherwise, both courts also questioned in those cases whether the government's actions were actually taken in "good faith," either because the affiant recklessly misled the court, *see United States v. Rice*, 478 F.3d 704, 709-11 (6th Cir. 2007); or because the wiretap order, in the court's view, plainly violated the applicable rule, *see United States v. Glover*, 736 F.3d 509, 515-16 (D.C. Cir. 2013). In this case, even if some aspect of the collection did not comply with the requirements of Section 702, there is no similar indication of deliberate, reckless, or systemically negligent conduct. Accordingly, absent a finding that the government personnel who carried out the collection did not rely in good faith on the targeting and minimization procedures as approved by the

III. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

A. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

B. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

C. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

c. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

d. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

e. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

f. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

FISC, or otherwise engaged in culpable conduct warranting application of the exclusionary rule, the defendant's motion to suppress should be denied.

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

D. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

E. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

4. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

F. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

IV. THE TRADITIONAL FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCHES WERE MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED INFORMATION REDACTED]

Furthermore, the FISA-authorized electronic surveillance and physical searches at issue in this case would fall squarely within the "good faith exception" discussed above. *See United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007) (holding that federal officers were entitled to rely in good faith on a FISA warrant); *see also United States v. Ahmed*, *No.1:06-CR-147,* 2009 U.S.

Dist. Lexis 120007 at *25 n.8, 26-27 (N. D. Ga. Mar. 19, 2009) ("[t]he FISA evidence obtained . . . would be admissible under *Leon*'s 'good faith' exception to the exclusionary rule were it not otherwise admissible under a valid warrant"). There is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *see also Massachusetts v. Sheppard*, 468 U.S. 981 (1984); *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000); *Duggan*, 743 F.2d at 77 n.6 (*Franks* principles apply to review of FISA orders). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the surveillance and searches at issue. *Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera, ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC's orders contained all of the requisite findings, and "well-trained officers" reasonably relied on those orders. Therefore, in the event that the Court questions whether a particular FISC order was supported by sufficient probable cause, the information obtained pursuant to those orders would be admissible under *Leon*'s "good faith" exception to the exclusionary rule. Accordingly, the Court should deny the defendant's motion.

A. STANDARD OF REVIEW

In evaluating the legality of the traditional FISA collection, the district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-131; *see also* 50 U.S.C. §§ 1806(f), 1825(g).

Although federal courts are not in agreement as to whether the probable cause determinations of the FISC should be reviewed *de novo* or accorded due deference, the Second Circuit has previously afforded due deference to the determination of the FISC and, in any event, the

material under review here satisfies either standard of review. *See Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review."); *accord, Ahmed*, 2009 U.S. Dist. Lexis 120007 at *21-22 (FISC's "determination of probable cause should be given 'great deference' by the reviewing court") (citing *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). The Government respectfully submits that this Court should accord due deference to the findings of the FISC.[60]

1. Probable Cause Standard

Traditional FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, or that the property or premises to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. It is this standard — not the standard applicable to criminal search warrants — that this Court must apply. *See El-Mezain*, 664 F.3d at 564 ("[t]his probable cause standard is different from the standard in the typical criminal case because, rather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power"); *Abu-Jihaad*, 630 F.3d at 130-31; *Duka*, 671 F.3d at 338; *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (citing

[60] A majority of Federal Courts have determined that the probable cause determination of the FISC should be reviewed *de novo*. *See United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005); *Rosen*, 447 F. Supp. 2d at 545; *United States v. Warsame*, 547 F. Supp. 2d 982, 990-91 (D. Minn. 2008) (explaining the required showing is "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . ., there is a fair probability" that the search will be fruitful (citing *Gates*, 462 U.S. at 238)); *United States v. Kashmiri*, 2010 WL 4705159, at *1 (N.D. Ill. Nov. 10, 2010); *United States v. Nicholson*, 2010 WL 1641167, *5 (D. Or. April 21, 2010) In each of these cases, the courts applied a *de novo* standard in reviewing the FISC's probable cause findings, and each court found the applications before it contained probable cause.

United States v. U.S. District Court (Keith), 407 U.S. 297, 322 (1972)). This "different, and arguably lower, probable cause standard . . . reflects the purpose for which FISA search orders are issued." *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *22.

2. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subjected only to minimal scrutiny by the courts," *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011) ("a presumption of validity [is] accorded to the certifications"); *Nicholson*, 2010 WL 1641167, at *5 (quoting *Rosen,* 447 F. Supp. 2d at 545); *Warsame*, 547 F. Supp. 2d at 990 ("a presumption of validity [is] accorded to the certifications"). When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.*; *see also In re Grand Jury Proceedings*, 347 F.3d 197, 204-05 (7th Cir. 2003); *Badia*, 827 F.2d at 1463; *United States v. Rahman*, 861 F. Supp. 247, 250 (S.D.N.Y. Aug. 18, 1994); *United States v. Islamic American Relief Agency*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009); *Kashmiri*, 2010 WL 4705159, at *1.

The district court's review should determine whether the certifications were made in accordance with FISA's requirements and, when the target is a United States person, that each certification is not "clearly erroneous."[61] *See United States v. Alwan,* No. 1:11-CR-13, 2012 WL

[61] [CLASSIFIED INFORMATION REDACTED]

399154, at *7 (W.D. Ky. Feb. 7, 2012) ("the [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made") (quoting *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *20); *see also Campa*, 529 F.3d at 993-94 ("in the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target") (quoting *Badia*, 827 F.2d at 1463); *Duggan*, 743 F.2d at 77; *Kashmiri*, 2010 WL 4705159, at *2. A "clearly erroneous" finding is established only when "although there is evidence to support [the issuing court's conclusion], the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *Islamic American Relief Agency*, 2009 WL 5169536, at *4 (identifying "clearly erroneous" standard of review for FISA certifications).

B. THE INSTANT FISA APPLICATIONS MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

i. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

ii. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

iii. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

i. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

ii. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

iii. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

iv. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. Conclusion: There Was Sufficient Probable Cause to Establish that the Information Acquired from the Targeted Facilities, Places, Property, or Premises Was Lawfully Acquired

[CLASSIFIED INFORMATION REDACTED]

C. THE CERTIFICATIONS COMPLIED WITH FISA

[CLASSIFIED INFORMATION REDACTED]

1. Foreign Intelligence Information

[CLASSIFIED INFORMATION REDACTED]

2. "A Significant Purpose"

[CLASSIFIED INFORMATION REDACTED]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED INFORMATION REDACTED]

For all of the above reasons, the FISC correctly found that the certifications were not clearly erroneous.

D. ALL ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCHES WERE CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

An *in camera, ex parte* review of the FISA materials will demonstrate not only that the FISA information was lawfully acquired, but also that the electronic surveillance and physical searches were lawfully conducted. That is, the FISA-obtained or -derived information that will be offered into evidence in this case was acquired, retained, and disseminated by the FBI in accordance with FISA's minimization requirements, and the standard minimization procedures ("SMPs") adopted by the Attorney General and approved by the FISC.

1. The Standard Minimization Procedures

Once a reviewing court is satisfied that the electronic surveillance or physical searches were properly certified and the information was lawfully acquired pursuant to FISA, it must then examine whether the electronic surveillance or physical searches were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to examine whether the electronic surveillance or physical searches were lawfully conducted, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED INFORMATION REDACTED]

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into

account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252-53. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741; *see also Bin Laden*, 126 F. Supp. 2d at 286 ("more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted" [internal quotation marks omitted]). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Matter of Kevork*, 634 F. Supp. 1002, 1017 (C.D. Cal. 1985) (quoting H.R. Rep. No. 95-1283, at 55 (1978) (hereinafter "House Report")); *see also Hammoud*, 381 F.3d at 334 (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41; *United States v. Thomson*, 752 F. Supp. 75, 81 (W.D.N.Y. 1990) (noting that it is permissible to retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing House

Report, part 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252-53 (citing House Report, part 1, at 55, 59). The Government must be given flexibility where the conversations are carried out in a foreign language. *Mubayyid*, 521 F. Supp. 2d at 134; *Rahman*, 861 F. Supp. at 252. As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report, part 1, at 58. Indeed, at least one court has cautioned that, when a U.S. person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *Cf. Thomson*, 752 F. Supp. at 81 (quoting House Report part 1, at 58). Accordingly, to pursue leads, Congress intended that the Government be given "a significant

degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." *Cf. Id.*

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, at 39 (quoting *Keith*, 407 U.S. at 323) (1978) ("Senate Report"). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136 (1978). "The test of compliance is 'whether a good-faith effort to minimize was made.'" *Mubayyid*, 521 F. Supp. 2d at 135; *see also Hammoud*, 381 F.3d at 334 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); *see also* Senate Report at 39-40 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion"); *Islamic American Relief Agency*, 2009 WL 5169536, at *6 (quoting Senate Report at 39-40).

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also United States v. Isa*, 923 F.2d. 1300,

1304 (8th Cir. 1991) (noting that "[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See Isa*, 923 F.2d. at 1300, 1305.

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED INFORMATION REDACTED]

Based upon this information, we respectfully submit that the Government lawfully conducted the FISA collections discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collections discussed herein were lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collections discussed herein.

V. THE DEFENDANT'S DISCOVERY MOTION SHOULD BE DENIED

Defendant renews (Def. Mot. 66-99) his motion, which he previously filed in the Section 2255 proceeding, for discovery of the classified materials relating to the authorization and conduct of the Section 702 and FISA collection. For the reasons set forth below and in the government's original response to defendant's discovery motion, defendant's request for discovery of classified material should be denied.

A. [CLASSIFIED INFORMATION REDACTED]

FISA provides that, where the Attorney General certifies that "disclosure [of FISA materials] or an adversary hearing would harm the national security of the United States," a district court "shall, notwithstanding any other law, . . . review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f).

This same procedure applies to motions related to Section 702 collection, which is deemed to be Title I FISA surveillance for purposes of such motions. 50 U.S.C. § 1881e(a). If the Attorney General files such a declaration, as he has done here, the district court must review the FISA materials *ex parte* and *in camera* and may disclose the applications and orders (or portions thereof) "only where such disclosure is *necessary* to make an accurate determination of the legality of the surveillance [or search]." *Id.* (emphasis added).

[CLASSIFIED INFORMATION REDACTED]

B. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

C. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

D. [CLASSIFIED INFORMATION REDACTED]

Defendant contends (Def. Mot. 69-74) that disclosure of the Section 702 and FISA materials is warranted because, he claims, adversarial procedures are a better mechanism for discovering truth than *in camera*, *ex parte* review by the court. However, that argument is contrary to Congress's judgment, embodied in FISA's text, that courts are to review Section 702 and FISA materials *ex parte* and *in camera* except when disclosure is necessary for the court to determine the legality of the surveillance. *See* 50 U.S.C. § 1806(f). Defendant's reliance on policy judgments is unavailing because they run counter to the balance Congress struck in devising FISA's suppression procedures. The advantages of the adversary process were not lost on Congress, but Congress weighed those benefits against the exceptionally high costs of revealing sensitive foreign intelligence information. *See Belfield*, 692 F.2d at 148 (noting that Congress was "aware" of the difficulties of *ex parte* procedures, but Congress nevertheless made a "thoroughly reasonable attempt to balance

the competing concerns of individual privacy and foreign intelligence."). If a defendant could obtain disclosure merely by pointing out that adversary procedures are generally beneficial and that such procedures would help him formulate his arguments more effectively, disclosure would become the norm, circumventing Congress's intentions and upsetting decades of case law. *See Abu-Jihaad*, 630 F.3d at 129 (recognizing that disclosure "is the exception" while "*ex parte, in camera* determination is the rule"); *Belfield*, 692 F.2d at 146-48 (noting that Congress "was adamant" that the "carefully drawn procedures" of § 1806(f) were not to be "bypassed by the inventive litigant using a new . . . judicial construction").

Contrary to defendant's argument, FISA's procedures strike a reasonable balance of competing interests, and have been held to be constitutional by every federal court that has considered the issue. *See, e.g.*, *El-Mezain*, 664 F.3d at 567-69; *United States v. Damrah*, 412 F.3d 618, 624-25 (6th Cir. 2005); *Belfield*, 692 F.2d at 147-48. In addition, the defendant's argument ignores the fact that courts have consistently upheld the use of *in camera, ex parte* review in various contexts, including specifically reviewing lawfulness of electronic surveillance. *See Kaley v. United States*, 134 S. Ct. 1090, 1103 (2014) (noting that the Supreme Court has "repeatedly declined to require the use of adversarial procedures to make probable cause determinations"); *United States v. Daoud*, 755 F.3d 479, 482 (7th Cir. 2014) (recognizing that many hearings in multiple contexts are properly conducted *ex parte*); *Taglianetti v. United States*, 394 U.S. 316, 317 (1969) ("Nothing [in the Supreme Court's preceding decisions] requires an adversary proceeding and full disclosure for resolution of every issue raised by an electronic surveillance"); *Giordano v. United States*, 394 U.S. 310, 313 (1969) ("[A] finding by the District Court that the surveillance was lawful would make disclosure and further proceedings unnecessary"); *id.* 314 (Stewart, J., concurring) ("We have nowhere indicated that this determination cannot appropriately be made in *in camera*, *ex parte*

proceedings."); *United States v. Ajlouny*, 629 F.2d 830, 839 (2d Cir. 1980) (holding that an adversary hearing and full disclosure are not required to resolve the legality of electronic surveillance "when the task is such that in camera procedures will adequately safeguard the defendant's Fourth Amendment rights"); *see also Alderman v. United States*, 394 U.S. 165, 184 n.15 (1969) (rejecting the principle that disclosure of the fruits of surveillance in lieu of *in camera* inspection is always required to adjudicate suppression motions regardless of the impact of disclosure on national security).[62] In accordance with these principles, the government's undeniable interest in protecting ongoing national security investigations and intelligence sources and methods, coupled with the protections found in other parts of Section 702 and FISA, justifies, as a matter of constitutional due process, FISA's limitations on the defendant's right to review the classified FISA and Section 702 materials. *See Daoud*, 755 F.3d at 483 (FISA's requirement of *in camera, ex parte* review "is an attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation"); *El-Mezain*, 664 F.3d at 567-69.

Defendant contends (Def. Mot. 75-76, 80) that alleged government misrepresentations in various other national security-related cases support ordering disclosure based on "possible misrepresentations of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information."

---

[62] Contrary to defendant's contention (Def. Mot. 70), *Alderman* does not support a constitutional requirement of full disclosure and an adversary hearing in this case. *See Ajlouny*, 629 F.3d at 839 (recognizing that the rationale of *Alderman* did not require disclosure in the context of foreign intelligence surveillance, even before FISA); *United States v. Bissell*, 634 F.2d 1228, 1232-33 (9th Cir. 1981) ("[N]othing in *Alderman* requires an adversary proceeding and full disclosure for resolution of every issue raised by an electronic surveillance"); *Damrah*, 412 F.3d at 624 (concluding that *Alderman* did not support disclosure of FISA materials or an adversary hearing and distinguishing *Alderman*, because, in that case, "the prosecution planned to use evidence from surveillance that had already been deemed unlawful").

However, defendant fails to recognize that, to justify disclosure, the court must first find that those factors are present with respect to the collection at issue in *this* case, after *ex parte*, *in camera* review. *See United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (noting that there are "no indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, or any other factors that would indicate a need for disclosure in *this case*) (internal quotation marks omitted) (emphasis added); *Warsame*, 547 F. Supp. 2d at 987-88 (noting that defendant's allegations that "the government has included misstatements and critical omissions in other FISA applications not at issue here cannot justify disclosure in this case"). As this Court's review of the classified record will show, there is no basis for a finding of material misrepresentations or other factors that would indicate a need for disclosure here.

Nor do the defendant's citations (Def. Mot. 47-60, 76) to statements in various FISC opinions, most of which do not involve Section 702, justify ordering disclosure of the Section 702 materials. Apart from the fact that those opinions have virtually no relevance to the present case, they underscore a more significant fact: the government takes its obligations under FISA and the Constitution seriously and candidly acknowledges and corrects deficiencies and compliance problems when it discovers them. *See* Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act (Jan. 10, 2014) at 5, 7 (noting that the government generally exhibits a "high degree of candor" in *ex parte* proceedings before the FISC and that the government "routinely discloses in an application information that is detrimental to its case"), available at www.judiciary.senate.gov/resources/documents/113thCongressDocuments/upload/011413RecordSub-Grassley.pdf; PCLOB Report at at 11 (finding "no trace" of any attempted "exploitation of information acquired under [Section 702] for illegitimate purposes" nor "any attempt to intentionally

circumvent legal limits"). To the extent that there are any issues concerning the lawfulness of the Section 702 collection at issue, as raised in FISC opinions, those have been addressed in this pleading. The defendant's speculation therefore cannot overcome the statutory presumption favoring this Court's *ex parte* review.[63]

[CLASSIFIED INFORMATION REDACTED]

At the outset, the balancing test proposed by the defendant "does not provide the appropriate framework" for assessing the constitutionality of the FISA procedures in the context of this criminal case. *See Medina v. California*, 505 U.S. 437, 443 (1992). As the Supreme Court stated in *Medina*, because the "Bill of Rights speaks in explicit terms to many aspects of criminal procedure," the expansion of procedures under an "open-ended" due process balancing analysis "invites undue interference with both considered legislative judgments and the careful balance that the Constitution strikes between liberty and order." *Id.* at 443. The Sixth Circuit has held, in a constitutional challenge to FISA's *ex parte, in camera* review procedures, that a defendant's reliance on a due process balancing test was "misplaced" because "FISA's requirement that the district court conduct an *ex parte*, *in camera* review of FISA materials does not deprive a defendant of due process." *Damrah*, 412 F.3d at 624.

Even assuming that a general due process balancing test applies here, the government's compelling interest in protecting against disclosure of national security information outweighs the defendant's interests, which are well protected by this court's *ex parte*, *in camera* review.

---

[63] [CLASSIFIED INFORMATION REDACTED]
[CLASSIFIED INFORMATION REDACTED]

The government's interest in protecting against disclosure of national security information is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *Ott*, 827 F.2d at 477.[64] Accordingly, as courts have recognized, confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information." *CIA v. Sims*, 471 U.S. 159, 175 (1985); *see also Phillippi v. CIA*, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). When considering whether the disclosure of classified sources, methods, techniques, or information would harm the national security, courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, when revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) ("each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself").

[64] The specific harms that would result from the disclosure of the FISA and Section 702 materials in this case are detailed in the classified documents in the Sealed Appendix.

For these reasons, defendant's argument (Def. Mot. 84-85) that various authorized and unauthorized disclosures of information related to government surveillance under Section 702 and other authorities have reduced the government's interest in protecting the classified FISA and Section 702 materials in this case is without merit. It is simply not the case that, because some classified information has been disclosed, the government could have no valid interest in protecting other related classified information from disclosure, or in protecting against official disclosure of classified information that was disclosed without authorization but not officially confirmed. To the contrary, courts have consistently recognized that the government has a substantial interest in protecting intelligence information. *See El-Mezain*, 664 F.3d at 567-68 (recognizing the government's "substantial interest in maintaining the secrecy of the [FISA] materials," and that this interest "extends not only to the contents of the materials but also to the appearance of confidentiality in the operation of the intelligence services").

Moreover, this Court should reject any argument that defense counsel's possession of a security clearance is relevant to determining whether disclosure of FISA or Section 702 materials is warranted. It is not. At the threshold, a "need to know" must exist before classified information may be disclosed, even to those who possess a security clearance.[65] That essential prerequisite is present in the context of FISA or Section 702 materials only where disclosure to defense counsel is "necessary" for a court to adjudicate the legality of the FISA collection. Should a court declare itself incapable of making the determination required by 50 U.S.C. § 1806(f) without the assistance of

[65] *See* Executive Order No. 13526, §§ 4.1(a), 6.1(dd), 75 Fed.Reg. 707, 720, 729 (Jan. 5, 2010), which requires that a "need to know" determination be made prior to the disclosure of classified information to anyone, including those who possess an appropriate security clearance. In *Baldrawi v. Dep't of Homeland Security*, 596 F. Supp. 2d 389, 400 (D. Conn. 2009), the court determined that even counsel who held a top secret security clearance did not have a "need to know," and therefore denied him access to classified documents.

defense counsel, then and only then could a defense counsel who holds a valid security clearance of the appropriate level have a "need to know" the classified FISA material.

As the Ninth Circuit held in *Ott*:

> [Defendant] next asserts that the *ex parte*, *in camera* proceeding violated due process in this case because his various attorneys all had high security clearances and therefore disclosure to them of the FISA materials would not entail or risk dissimilation of sensitive information to non-cleared personnel. This argument is also unpersuasive. Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in the surveillance operation in question, whether or not she happens for unrelated reason to enjoy a security clearance. We reject the notion that a defendant's due process right to disclosure of FISA materials turns on the qualifications of his counsel.

827 F.2d at 476-77; *accord Nicholson*, 2010 WL 1641167, at *5 (referencing *Ott* and holding that "[b]ased on [the court's] *in camera* review...the disclosure of FISA materials to [cleared] defense counsel is neither required nor appropriate").

As mentioned above, the Seventh Circuit recently reversed a district court's finding that "any concerns about disclosure [of FISA material] were dissolved by defense counsel's security clearance." *Daoud*, 755 F.3d at 484-85. Rather, "[u]nless and until a district court judge performs his or her statutory duty of attempting to determine the legality of the surveillance without revealing any of the fruits of the surveillance to defense counsel, there is no basis for concluding that disclosure is necessary in order to avert an erroneous conviction." *Id.*; *accord United States v. Amawi*, 2009 WL 961143, at *1 (N.D. Ohio, April 7, 2009).

As the *Daoud* court noted, the simple possession of a security clearance does not automatically entitle its possessor to access any classified information of a level that he is cleared to see. *Daoud*, 755 F.3d at 484. As the court explained, the "need to know" requirement is a check against unwarranted disclosure of classified materials and thus "if the district court's threshold

inquiry into whether [defense counsel] needed any of the surveillance materials revealed that they didn't, their security clearances would not entitle them to any of those materials." *Id.* The court recognized that there are sound reasons underlying the "need to know" requirement, including the possibility that even cleared defense counsel "might in their zeal to defend their client, to whom they owe a duty of candid communication, or misremembering what is classified and what not, inadvertently say things that would prove clues to classified material." *Daoud*, 755 F.3d at 484; *see also id.* ("There are too many leaks of classified information—too much carelessness and irresponsibility in the handling of such information—to allow automatic access to holders of the applicable security clearances.").

Defendant's contention (Def. Mot. 85-95) that the due process balance favors disclosure relies on (1) the general benefits of the adversary system; (2) the complexity of the issues; and (3) alleged misrepresentations to the FISC. However, as explained above, these factors in no way undermine this Court's ability to determine the legality of the surveillance based on the *ex parte*, *in camera* process FISA requires. Accordingly, courts have uniformly held that "*in camera* and *ex parte* review by the district court adequately ensure[s] that the defendants' statutory and constitutional rights [a]re not violated." *El-Mezain*, 664 F.3d at 567; *see also Belfield*, 692 F.2d at 149 n.38 (disclosure of FISA materials is not constitutionally required because "*in camera* procedures will adequately safeguard [the defendant's] rights"); *ACLU Found. of Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (FISA's procedures are "an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance"). Thus, contrary to defendant's arguments, there is no reason to doubt that this Court's *in camera*, *ex parte* review will adequately protect defendant's constitutional rights.

Finally, defendant contends (Def. Mot. 95-96) that the Court should order disclosure of the classified FISA and Section 702 materials because adversarial process in this context would serve "important societal purposes of transparency and deterrence." Defendant's argument disregards the government's countervailing national security interests, as well as the conclusion of every court to have considered the issue that FISA's *ex parte*, *in camera* process represents a constitutionally reasonable "balance" of the "competing concerns of individual privacy and foreign intelligence." *Belfield*, 692 F.2d at 148. *See also Daoud*, 755 F.3d at 483 (explaining that FISA appropriately balances "the interest in full openness of legal proceedings" in "recognition of valid social interests" in preserving the "secrecy" which is necessary to "the government's efforts to protect the nation").[66]

Hasbajrami also renews (Def. Mot. 68, 96-97) his request for notice of "other surveillance programs" that he speculates may have been used in the government's investigation. As the government explained in its response to Hasbajrami's previous discovery motion (Gov't Opposition to Motion to Compel Discovery (Docket Entry 25) at 38), none of the other legal

---

[66] The defendant suggests (Def. Mot. 84) that disclosure of the classified FISA and Section 702 materials is required under *Brady v. Maryland*, 373 U.S. 83 (1963). The government understands and has every intention of complying with its discovery obligations. The defendant is not entitled to go on a "fishing expedition" of the government's files on the mere supposition that they may contain exculpatory information.

The due process requirement embraced by FISA is coterminous with the *Brady* standard. See *United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa. 1989). However, contrary to the defendant's speculation, none of the Section 702 materials submitted herewith are "material" within the meaning of *Brady*. The defendant's argument that due process requires disclosure of FISA materials based on his allegation that the materials likely will assist him in litigating his suppression motion would, again, apply in every FISA case and is therefore inconsistent with the numerous cases upholding FISA's *ex parte* review procedure against constitutional challenges. *See, e.g., El-Mezain*, 664 F.3d at 567-69; *Damrah*, 412 F.3d at 624-25; *Isa*, 923 F.2d at 1306-07; *Ott*, 827 F.2d at 476-77; *Belfield*, 692 F.2d at 148. Likewise, even if, as the defendant contends (Def. Mot. 83-84), FISA's due process disclosure requirement incorporates the "relevant and helpful" standard from the CIPA context, rather than the more stringent *Brady* standard, the Section 702 materials are not discoverable under either standard.

authorities or investigative activities raised in Hasbajrami's motions is relevant to this case. The government is aware of its discovery obligations and will provide the defense with all discoverable material in its possession or will address that material to this Court through the Classified Information Procedures Act (CIPA). Hasbajrami's unfounded speculation regarding other surveillance activities does not entitle him to any further discovery.

VI. THE DEFENDANT IS NOT ENTITLED TO A HEARING UNDER *FRANKS v. DELAWARE*

To the extent the defendant intends to argue that he is entitled to a *Franks* hearing based on purported misrepresentations or material falsehoods in any of the FISA applications in this case, (Def. Mot. 73), the court should deny this request.

When a defendant makes the requisite showing, the Court may conduct a *Franks* hearing to determine if there are material misrepresentations of fact, or omissions of material fact, before the FISC sufficient to warrant suppression of evidence obtained or derived from Title I and Title III FISA collections. *See Franks*, 438 U.S. at 171; *Ning Wen*, 477 F.3d at 897. To merit a *Franks* hearing, the defendant first must make a "concrete and substantial preliminary showing" that: (1) the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit; and (2) the misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155-56; *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990); *Duggan*, 743 F.2d at 77 & n.6; *Kashmiri*, 2010 WL 4705159, at *5 (defendant "has not made any showing – let alone a substantial one – that an Executive Branch officer knowingly and intentionally, or recklessly, included a false statement in the FISA application [and w]ithout such a showing, he is foreclosed from obtaining a hearing"). Failure of the defendant "to satisfy either of these two prongs proves fatal to a *Franks* hearing." *Id.* at *5; *Mubayyid*, 521 F. Supp. 2d at 130-31.

The defendant's burden in establishing the need for a *Franks* hearing is a heavy one. *United States v. Jeffus*, 22 F.3d 554, 558 (4th Cir. 1994). The defendant must submit allegations of deliberate falsehood or of reckless disregard for the truth, accompanied by an offer of proof. *Franks*, 438 U.S. at 171. Allegations of negligence or innocent mistake are insufficient, *id.*, as are allegations of insignificant or immaterial misrepresentations or omissions. *Colkley*, 899 F. 2d at 301-02. Moreover, a defendant's lack of access to the FISA applications and orders is not an adequate substitute for the required showing. Although this situation presents a quandary for defense counsel when FISA-derived evidence comes into play, Congress and the courts have recognized that such difficulty does not justify the disclosure of FISA materials:

> We appreciate the difficulties of appellants' counsel in this case. They must argue that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary. But without access to the relevant materials their claim of complexity can be given no concreteness. It is pure assertion.
>
> Congress was also aware of these difficulties. But it chose to resolve them through means other than mandatory disclosure. In FISA Congress has made a thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence . . . . Appellants are understandably reluctant to be excluded from the process whereby the legality of a surveillance by which they were incidentally affected is judged. But it cannot be said that this exclusion rises to the level of a constitutional violation.

Belfield, 692 F.2d at 148; *see also Kashmiri,* 2010 WL 4705159, at *6:

> Nevertheless, to challenge the veracity of the FISA application, Defendant must offer substantial proof that the FISC relied on an intentional or reckless misrepresentation by the government to grant the FISA order. The quest to satisfy the *Franks* requirements might feel like a wild-goose chase, as Defendant lacks access to the materials that would provide this proof. This perceived practical impossibility to obtain a hearing, however, does not constitute a legal impossibility.
>
> Moreover, other courts have rejected similar attempts by defendants to force a *Franks* hearing challenging the validity of FISA orders based on speculation. *See Mohamud, 2014 WL*

2866749, at *30-*31 (noting that the court "has already undertaken a process akin to a *Franks* hearing through its *ex parte, in camera* review"); *Abu-Jihaad*, 531 F. Supp. 2d at 310; *United States v. Hassoun*, No. 04-CR-60001, 2007 WL 1068127, at *4 (S.D. Fla. Apr. 4, 2007); *Mubayyid,* 521 F. Supp. 2d at 130-31. For example, citing prior instances of purported government misrepresentations or omissions in other cases or contexts does not satisfy the *Franks* standard "as it sheds no light on the truth or falsity of the particular FISA application under review." *Daoud*, 755 F.3d at 492 (Rovner, J. concurring).[67]

In sum, the defendant has failed to carry this burden of establishing the prerequisites for a *Franks* hearing, and there is no other basis that would support holding a *Franks* hearing. For these reasons, the Court should therefore deny any defense request for a *Franks* hearing and his request for disclosure of the FISA materials.

[67] Judge Rovner concurred in the *Daoud* court's opinion in full, but wrote separately to address the difficulty faced by defense counsel in mounting a *Franks* challenge under FISA's *ex parte*, *in camera* review standard. *Id.* at 485. While stating her belief that defendants in cases involving motions to suppress FISA evidence face a "virtually insurmountable obstacle" when seeking a *Franks* hearing without having access to the FISA materials, Judge Rovner properly recognized that disclosure of FISA materials to defense counsel and holding an adversary hearing would potentially risk national security and further noted that access to FISA materials would not necessarily help mount a *Franks* challenge because counsel would not be authorized to disclose them to the defendant. *Id.* at 490, 493. Ultimately, Judge Rovner recommended consideration, in the appropriate cases, of alternate *ex parte* methods to assess the veracity of allegations contained in FISA materials. In this case, however, there is no reason to engage in such steps.

VII. CONCLUSION

Based on the above discussion and analysis, the government requests that the Court deny defendant Hasbajrami's Motions No. 1, 2, and 5 contained in his Pretrial Omnibus Motions and Incorporated Memorandum of Law in Support Thereof.

Respectfully submitted,

LORETTA E. LYNCH
United States Attorney
Eastern District of New York

By: /s/
Seth D. DuCharme
Matthew S. Amatruda
Saritha Komatireddy
Assistant U.S. Attorneys
Eastern District of New York

JOHN P. CARLIN
Assistant Attorney General
For National Security

By: /s/
Danya E. Atiyeh
Kiersten Korczynski
Trial Attorneys
Counterterrorism Section
Department of Justice
(Of Counsel)